Redes de vSphere

Actualización 2
Modificada el 19 abril de 2022
VMware vSphere 6.5
VMware ESXi 6.5
vCenter Server 6.5

Puede encontrar la documentación técnica más actualizada en el sitio web de VMware:

https://docs.vmware.com/es/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware Spain, S.L.
Calle Rafael Boti 26
2.ª planta
Madrid 28023
Tel.: +34 914125000
www.vmware.com/es

Contenido

Acerca de las redes de vSphere

Redes de vSphere proporciona información sobre la configuración de redes para VMware vSphere®, incluida información sobre cómo crear conmutadores distribuidos de vSphere y conmutadores estándar de vSphere.

Las redes vSphere también proporcionan información sobre la supervisión de redes, la administración de los recursos de la red y las prácticas recomendadas de redes.

Audiencia prevista

La información se presenta para los administradores de sistemas con experiencia en Windows o en Linux que están familiarizados con la configuración de red y con las tecnologías de las máquinas virtuales.

vSphere Web Client y vSphere Client

Las instrucciones para las tareas en esta guía se basan en vSphere Web Client. También puede realizar la mayoría de las tareas en esta guía con la nueva instancia de vSphere Client. La terminología, la topología y el flujo de trabajo de la interfaz de usuario de la nueva instancia de vSphere Client están estrechamente alineados con los mismos aspectos y elementos de la interfaz de usuario de vSphere Web Client. Puede aplicar las instrucciones de vSphere Web Client a la nueva instancia de vSphere Client, a menos que se indique lo contrario.

Nota No todas las funcionalidades de vSphere Web Client se implementaron para vSphere Client en la versión de vSphere 6.5. Para obtener una lista actualizada de las funcionalidades no compatibles, consulte la *Guía sobre actualizaciones de las funcionalidades en vSphere Client* en http://www.vmware.com/info?id=1413.

Información actualizada

Estas *redes de vSphere* se actualizan con cada versión del producto o cuando es necesario.

En esta tabla se muestra el historial de actualizaciones de las *redes de vSphere*.

Revisión	Descripción
25 ENE 2022	Se agregó una nota sobre las limitaciones al seleccionar los orígenes de creación de reflejo del puerto. Consulte Seleccionar orígenes de creación de reflejo del puerto.
31 de marzo de 2021	Actualizaciones varias.
13 de abril de 2020	Se amplió la descripción de la comprobación de estado de vSphere Distributed Switch para incluir la recomendación de uso por la cual se aconseja utilizar la comprobación de estado para solucionar problemas de red y, después de identificar y resolver el problema, deshabilitarla. Consulte Comprobar estado de vSphere Distributed Switch y Habilitar o deshabilitar la comprobación de estado de vSphere Distributed Switch.
13 de abril de 2020	Se actualizaron los patrones para filtrar o marcar el tráfico de red mediante una dirección MAC, para eliminar el uso de una expresión regular con comodines. Se considera que una dirección MAC coincide si la operación Y de la máscara en la dirección MAC produce el mismo resultado. Consulte Calificador de tráfico de MAC.
13 de abril de 2020	Versión inicial.

Introducción a las redes

1

Se analizan los conceptos básicos de redes de ESXi y la configuración de una red en un entorno de vSphere.

Este capítulo incluye los siguientes temas:

Descripción general de los conceptos de redes

Algunos conceptos son esenciales para una comprensión integral de las redes virtuales. Si es su primera vez con ESXi, será útil revisar estos conceptos.

Red física

Red de máquinas físicas que están conectadas para poder enviar y recibir datos entre sí. VMware ESXi se ejecuta en una máquina física.

Red virtual

Red de máquinas virtuales que se ejecutan en una máquina física y que están interconectadas de manera lógica para poder enviar y recibir datos entre sí. Las máquinas virtuales pueden conectarse a las redes virtuales que se crean cuando se agrega una red.

Red opaca

Una red opaca es una red creada y administrada por una entidad independiente externa a vSphere. Por ejemplo, las redes lógicas que crea y administra VMware NSX ® aparecen en vCenter Server como redes opacas del tipo nsx.LogicalSwitch. Una red opaca se puede elegir como copia de seguridad para un adaptador de red de máquina virtual. Para administrar una red opaca, use las herramientas de administración relacionadas con la red opaca, como VMware NSX® Manager™ o VMware NSX® API™.

Conmutador Ethernet físico

Administra el tráfico de red entre las máquinas de la red física. Un conmutador tiene varios puertos, cada uno de los cuales se puede conectar a una sola máquina o a otro conmutador en

la red. Cada puerto puede configurarse para que se comporte de ciertas maneras en función de las necesidades de la máquina conectada a él. El conmutador determina qué hosts están conectados a cuáles de sus puertos y utiliza esa información para enviar tráfico a las máquinas físicas correctas. Los conmutadores son el núcleo de una red física. Varios conmutadores pueden conectarse entre sí para formar redes más grandes.

Conmutador estándar de vSphere

Funciona como un conmutador Ethernet físico. Detecta qué máquinas virtuales están conectadas de manera lógica a cada uno de sus puertos virtuales y utiliza esa información para enviar tráfico a las máquinas virtuales correctas. Para unir redes virtuales con redes físicas, un conmutador estándar de vSphere se puede conectar a conmutadores físicos mediante el uso de adaptadores Ethernet físicos, también conocidos como adaptadores de vínculo superior. Este tipo de conexión es similar a la conexión de conmutadores físicos entre sí para crear una red más grande. A pesar de que un conmutador estándar de vSphere funciona como un conmutador físico, no tiene algunas de las funcionalidades avanzadas de un conmutador físico.

Grupo de puertos estándar

Especifica las opciones de configuración de puertos, como las limitaciones de ancho de banda y las directivas de etiquetado de VLAN para cada puerto miembro. Los servicios de red se conectan a conmutadores estándar a través de grupos de puertos. Los grupos de puertos definen cómo se realiza una conexión con la red a través del conmutador. Por lo general, un solo conmutador estándar se asocia con uno o más grupos de puertos.

vSphere Distributed Switch

Actúa como un solo conmutador en todos los hosts asociados en un centro de datos para proporcionar administración, supervisión de redes virtuales y aprovisionamiento centralizado. Es posible configurar un conmutador distribuido de vSphere en el sistema vCenter Server y la configuración se completa a través de todos los hosts que están asociados al conmutador. Esto permite que las máquinas virtuales mantengan una configuración de red coherente a medida que migran a varios hosts.

Conmutador proxy del host

Conmutador estándar oculto que reside en cada host que está asociado a un conmutador distribuido de vSphere. El conmutador proxy del host replica la configuración de redes establecida en el conmutador distribuido de vSphere a ese host en particular.

Puerto distribuido

Puerto en un conmutador distribuido de vSphere que se conecta al VMkernel de un host o al adaptador de red de una máquina virtual.

Grupo de puertos distribuidos

Grupo de puertos que se asocia a un conmutador distribuido de vSphere y especifica las opciones de configuración de puerto que corresponden a cada puerto miembro. Los grupos

de puertos distribuidos definen cómo se establece una conexión con la red a través del conmutador distribuido de vSphere a la red.

Formación de equipos de NIC

La formación de equipos de NIC se produce cuando varios adaptadores de vínculo superior se asocian a un solo conmutador para formar un equipo. Un equipo puede compartir la carga de tráfico entre redes físicas y virtuales con todos o algunos de sus miembros, o bien proporcionar conmutación por error pasiva en caso de un error de hardware o un corte de red.

VLAN

VLAN permite que se segmente un único segmento LAN físico para que los grupos de puertos queden aislados unos de otros como si estuvieran en segmentos físicamente diferentes. El estándar es 802.1Q.

Capa de redes de VMkernel TCP/IP

La capa de redes VMkernel proporciona conectividad a los hosts y controla el tráfico de infraestructura estándar de vSphere vMotion, almacenamiento IP, Fault Tolerance y vSAN.

Almacenamiento IP

Cualquier forma de almacenamiento que utiliza como base una comunicación de red TCP/IP. iSCSI se puede usar como un almacén de datos de la máquina virtual, y NFS se puede utilizar como un almacén de datos de una máquina virtual y para el montaje directo de archivos de `.ISO`, que se presentan a las máquinas virtuales como CD-ROM.

descarga de segmentación de TCP

La descarga de segmentación de TSO permite que una pila de TCP/IP emita grandes tramas (hasta 64 KB) a pesar de que la unidad de transmisión máxima (MTU) de la interfaz sea más pequeña. El adaptador de red, a continuación, separa la trama grande en tramas del tamaño de la MTU y antepone una copia ajustada de los encabezados de TCP/IP.

Servicios de red en ESXi

Una red virtual proporciona varios servicios al host y a las máquinas virtuales.

Se pueden habilitar dos tipos de servicios de red en ESXi:

- Conexión de las máquinas virtuales a la red física y entre ellas.
- Conexión de los servicios VMkernel (como NFS, iSCSI o vMotion) a la red física.

Compatibilidad con VMware ESXi Dump Collector

ESXi Dump Collector envía el estado de la memoria VMkernel, es decir, envía un volcado de núcleo a un servidor de red cuando el sistema encuentra un error grave.

ESXi Dump Collector en ESXi 5.1 y versiones posteriores admiten vSphere Standard Switch y vSphere Distributed Switch. ESXi Dump Collector también puede utilizar cualquier adaptador de vínculo superior activo del equipo del grupo de puertos que controla el adaptador VMkernel del recopilador.

Los cambios en la dirección IP de la interfaz de ESXi Dump Collector se actualizan automáticamente si cambia la dirección IP del adaptador VMkernel configurado. ESXi Dump Collector también ajusta su puerta de enlace predeterminada si cambia la configuración de la puerta de enlace del adaptador VMkernel.

Si se intenta eliminar el adaptador de red VMkernel utilizado por ESXi Dump Collector, la operación falla y aparece un mensaje de advertencia. Para eliminar el adaptador de red VMkernel, deshabilite la recopilación en volcado y elimine el adaptador.

No hay autenticación ni cifrado en la sesión de transferencia de archivos desde un host bloqueado hacia ESXi Dump Collector. Se debe configurar ESXi Dump Collector en una VLAN distinta cuando sea posible, a fin de aislar el volcado de núcleo de ESXi del tráfico de red.

Para obtener información sobre cómo instalar y configurar ESXi Dump Collector, consulte la documentación de *Instalar y configurar vCenter Server*.

Configurar redes con vSphere Standard Switch

2

vSphere Standard Switch controla el tráfico de red en el nivel de host en una implementación de vSphere.

Este capítulo incluye los siguientes temas:

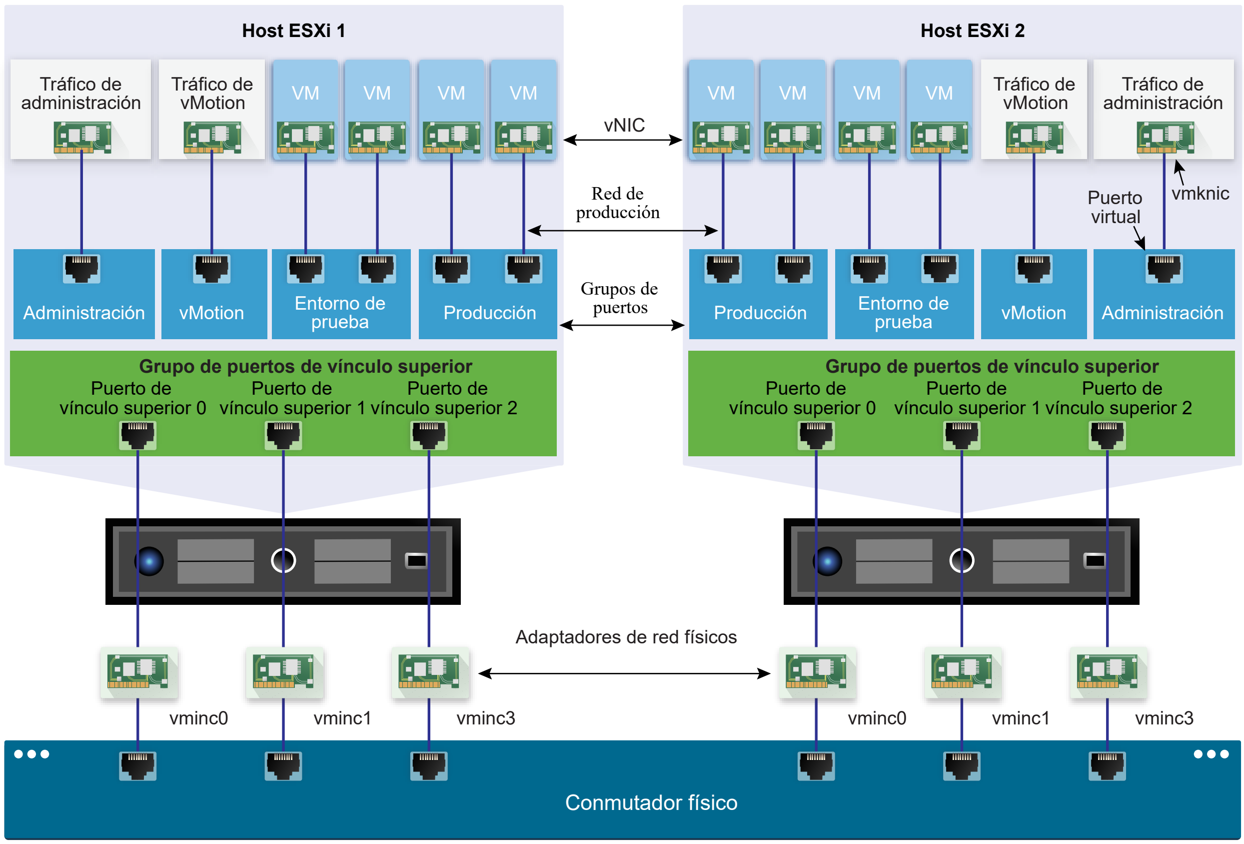
vSphere Standard Switch

Puede crear dispositivos de red abstractos denominados vSphere Standard Switch. Estos conmutadores se utilizan para brindar conectividad de red a los hosts y las máquinas virtuales. Un conmutador estándar puede actuar como puente interno para el tráfico entre las máquinas virtuales de una misma VLAN y como vínculo para las redes externas.

Descripción general del conmutador estándar

Para brindar conectividad de red a los hosts y las máquinas virtuales, conecte las NIC físicas de los hosts a los puertos de vínculo superior en el conmutador estándar. Las máquinas virtuales tienen adaptadores de red (vNIC) que se conectan a los grupos de puertos en el conmutador estándar. Cada grupo de puertos puede utilizar una o varias NIC físicas para controlar su tráfico de red. Si un grupo de puertos no tiene una NIC física conectada, las máquinas virtuales del mismo grupo de puertos solo pueden comunicarse entre sí, pero no con la red externa.

Figura 2-1. Arquitectura de vSphere Standard Switch



vSphere Standard Switch es muy similar a un conmutador físico de Ethernet. Los adaptadores de red de máquina virtual y las NIC virtuales del host utilizan los puertos lógicos del conmutador, ya que cada adaptador utiliza un puerto. Cada puerto lógico del conmutador estándar es miembro de un solo grupo de puertos. Para obtener información sobre la cantidad máxima permitida de puertos y grupos de puertos, consulte la documentación de *Valores máximos de configuración*.

Grupos de puertos estándar

Cada grupo de puertos de un conmutador estándar se identifica por una etiqueta de red, que debe ser exclusiva del host actual. Puede utilizar las etiquetas de red para que la configuración de redes de las máquinas virtuales se pueda trasladar de un host a otro. Aplique la misma etiqueta a los grupos de puertos de un centro de datos que utilice las NIC físicas conectadas a un dominio de difusión en la red física. En cambio, si hay dos grupos de puertos conectados a NIC físicas en diferentes dominios de difusión, los grupos de puertos deben tener etiquetas diferentes.

Por ejemplo, puede crear grupos de puertos *Production* y *Test environment* como redes de máquina virtual en los hosts que comparten el mismo dominio de difusión en la red física.

De forma opcional, se puede incluir un identificador de VLAN, que restringe el tráfico del grupo de puertos a un segmento lógico de Ethernet dentro de la red física. Para que los grupos de puertos reciban el tráfico que ve el mismo host, pero desde más de una VLAN, el identificador de VLAN debe estar configurado como VGT (VLAN 4095).

Cantidad de puertos estándar

Para asegurar un uso eficiente de los recursos en los hosts que ejecutan ESXi 5.5 y versiones posteriores, la cantidad de puertos de los conmutadores estándar se escala dinámicamente de forma vertical y horizontal. Un conmutador estándar de este tipo de host puede expandirse hasta la cantidad máxima de puertos admitida por el host.

Crear vSphere Standard Switch

Cree vSphere Standard Switch para ofrecer conectividad de red a los hosts y las máquinas virtuales, y para manejar el tráfico de VMkernel. Según el tipo de conexión que desee crear, puede crear vSphere Standard Switch con un adaptador VMkernel, conectar únicamente los adaptadores de red físicos al nuevo conmutador o crear el conmutador con un grupo de puertos de máquina virtual.

Procedimiento

1 En vSphere Web Client, desplácese hasta el host.

2 En la pestaña **Configurar**, expanda **Redes** y seleccione **Conmutadores virtuales**.

3 Haga clic en **Agregar redes de host**.

4 Seleccione el tipo de conexión para el cual desea usar el nuevo conmutador estándar y haga clic en **Siguiente**.

Opción	Descripción
Adaptador de red VMkernel	Cree un nuevo adaptador VMkernel para manejar el tráfico de administración de host, vMotion, el almacenamiento de red, la tolerancia a errores o el tráfico de vSAN.
Adaptador de red físico	Agregue adaptadores de red físicos a un conmutador estándar existente o nuevo.
Grupo de puertos de máquina virtual para un conmutador estándar	Cree un nuevo grupo de puertos para la conexión en red de máquinas virtuales.

5 Seleccione **Nuevo conmutador estándar** y haga clic en **Siguiente**.

6 Agregue adaptadores de red físicos al nuevo conmutador estándar.

a En Adaptadores asignados, haga clic en **Agregar adaptadores**.

b Seleccione uno o varios adaptadores de red físicos de la lista.

c En el menú desplegable **Grupo de orden de conmutación por error**, seleccione opciones de las listas de conmutación Activa o En espera.

Si desea mejorar la capacidad de proceso y disponer de redundancia, configure al menos dos adaptadores de red físicos en la lista Activa.

d Haga clic en **Aceptar**.

7 Si crea un conmutador estándar nuevo con un adaptador VMkernel o un grupo de puertos de máquina virtual, introduzca la configuración de conexión del adaptador o del grupo de puertos.

Opción	Descripción
adaptador VMkernel	a Introduzca una etiqueta que identifique el tipo de tráfico para el adaptador VMkernel, por ejemplo **`vMotion`**. b Establezca un identificador de VLAN para identificar la VLAN que utilizará el tráfico de red del adaptador VMkernel. c Seleccione IPv4, IPv6 o ambas opciones. d Seleccione una pila de TCP/IP. Después de establecer una pila de TCP/IP para el adaptador VMkernel, no es posible cambiarla más adelante. Si selecciona vMotion o la pila de TCP/IP de aprovisionamiento, podrá utilizar solo esta pila para controlar vMotion o el tráfico de aprovisionamiento en el host. e Si usa la pila de TCP/IP predeterminada, seleccione los servicios disponibles que desee. f Configure las opciones de IPv4 e IPv6.
Grupo de puertos de máquina virtual	a Introduzca una etiqueta de red para el grupo de puertos o acepte la etiqueta generada. b Establezca el identificador de la VLAN para configurar el manejo de la VLAN en el grupo de puertos.

8 En la página Listo para finalizar, haga clic en **Aceptar**.

Pasos siguientes

- Puede que sea necesario cambiar la directiva de formación de equipos y conmutación por error del nuevo conmutador estándar. Por ejemplo, si el host está conectado a un EtherChannel en el conmutador físico, vSphere Standard Switch debe configurarse con Route Enrutar según el hash de IP como algoritmo de equilibrio de carga. Consulte Directiva de formación de equipos y conmutación por error para obtener más información.
- Si crea el nuevo conmutador estándar con un grupo de puertos para la conexión en red de máquinas virtuales, conecte las máquinas virtuales al grupo de puertos.

Configurar un grupo de puertos para máquinas virtuales

Es posible agregar o modificar un grupo de puertos de máquina virtual para configurar la administración de tráfico en un conjunto de máquinas virtuales.

El asistente **Agregar redes** de vSphere Web Client funciona como guía en el proceso de creación de una red virtual a la que se puedan conectar las máquinas virtuales. Este proceso incluye la creación de vSphere Standard Switch y la configuración de una etiqueta de red.

Al configurar redes de máquinas virtuales, considere si desea migrar las máquinas virtuales de la red entre los hosts. Si así fuera, asegúrese de que ambos hosts se encuentren en el mismo dominio de difusión, es decir, en la misma subred de Capa 2.

ESXi no admite la migración de máquinas virtuales entre hosts de diferentes dominios de difusión, ya que la máquina virtual migrada puede requerir sistemas y recursos a los que es posible que ya no tenga acceso desde la nueva red. Incluso si la configuración de red se establece como un entorno de alta disponibilidad o incluye conmutadores inteligentes que pueden resolver las necesidades de la máquina virtual en diferentes redes, se pueden producir tiempos de retardo debido a que la tabla de Address Resolution Protocol (ARP) actualiza y reanuda el tráfico de red para las máquinas virtuales.

Las máquinas virtuales alcanzan redes físicas a través de los adaptadores de vínculo superior. vSphere Standard Switch puede transferir datos a redes externas solo si se conecta un adaptador de red, o varios, a él. Cuando se conectan dos o más adaptadores a un único conmutador estándar, se agrupan de manera transparente.

Agregar un grupo de puertos de máquina virtual

Cree grupos de puertos en vSphere Standard Switch para proporcionar conectividad y configuración de red común a las máquinas virtuales.

Procedimiento

1 En vSphere Web Client, desplácese hasta el host.

2 Haga clic con el botón derecho en el host y seleccione **Agregar redes**.

3 En **Seleccionar tipo de conexión**, seleccione **Grupo de puertos de máquina virtual para conmutador estándar** y haga clic en **Siguiente**.

4 En **Seleccionar dispositivo de destino**, seleccione un conmutador estándar existente o cree uno nuevo.

5 Si el nuevo grupo de puertos es para un conmutador estándar existente, desplácese hasta el conmutador.

   a Haga clic en **Examinar**.

   b Seleccione un conmutador estándar de la lista y haga clic en **Aceptar**.

   c Haga clic en **Siguiente** y vaya a Paso 7.

6 (opcional) En la página Crear un conmutador estándar, asigne los adaptadores de red físicos al conmutador estándar.

   Es posible crear un conmutador estándar con o sin adaptadores.

Si crea un conmutador estándar sin adaptadores de red físicos, todo el tráfico del conmutador queda limitado a ese conmutador. Ninguno de los demás hosts de la red física o las máquinas virtuales de otros conmutadores estándar pueden enviar ni recibir tráfico a través de este conmutador estándar. Puede crear un conmutador estándar sin adaptadores de red físicos si desea que un grupo de máquinas virtuales puedan comunicarse entre sí, pero no con otros hosts o con máquinas virtuales fuera del grupo.

a Haga clic en **Agregar adaptadores**.

b Seleccione un adaptador de la lista **Adaptadores de red**.

c Utilice el menú desplegable **Grupo de orden de conmutación por error** para asignar el adaptador a adaptadores activos, adaptadores en espera o adaptadores sin usar, y haga clic en **Aceptar**.

d (opcional) Utilice las flechas hacia arriba y hacia abajo en la lista **Adaptadores asignados** para cambiar la posición del adaptador si fuera necesario.

e Haga clic en **Siguiente**.

7 En la página Configuración de conexión, identifique el tráfico a través de los puertos del grupo.

a Escriba una **Etiqueta de red** para el grupo de puertos o acepte la etiqueta generada.

b Establezca el valor de **Identificador de VLAN** para configurar el manejo de VLAN en el grupo de puertos.

El identificador de VLAN también refleja el modo de etiquetado de VLAN en el grupo de puertos.

Modo de etiquetado de VLAN	identificador de VLAN	Descripción
Etiquetado de conmutador externo (EST)	0	El conmutador virtual no transmite tráfico asociado con una VLAN.
Etiquetado de conmutador virtual (VST)	De 1 a 4094	El tráfico de etiquetas de conmutadores virtuales con la etiqueta introducida.
Etiquetado de conmutador invitado (VGT)	4095	Las máquinas virtuales controlan las VLAN. El conmutador virtual transmite tráfico desde cualquier VLAN.

c Haga clic en **Siguiente**.

8 Revise la configuración del grupo de puertos en la página Listo para finalizar y haga clic en **Finalizar**.

Haga clic en **Atrás** si desea cambiar alguna opción de configuración.

Editar un grupo de puertos del conmutador estándar

Al utilizar vSphere Web Client, es posible editar el nombre y el identificador de VLAN de un grupo de puertos del conmutador estándar, y reemplazar las directivas de redes en el grupo de puertos.

Procedimiento

1 En vSphere Web Client, desplácese hasta el host.

2 En la pestaña **Configurar**, expanda **Redes** y seleccione **Conmutadores virtuales**.

3 Seleccione de la lista un conmutador estándar.

Aparece el diagrama de topología del conmutador.

4 En el diagrama de topología del conmutador, haga clic en el nombre del grupo de puertos.

5 Debajo del título del diagrama de topología, haga clic en el icono **Editar configuración**.

6 En la página Propiedades, cambie el nombre del grupo de puertos en el campo de texto **Etiqueta de red**.

7 Configure el etiquetado de VLAN en el menú desplegable **identificador de VLAN**.

Modo de etiquetado de VLAN	identificador de VLAN	Descripción
Etiquetado de conmutador externo (EST)	0	El conmutador virtual no transmite tráfico asociado con una VLAN.
Etiquetado de conmutador virtual (VST)	De 1 a 4094	El tráfico de etiquetas de conmutadores virtuales con la etiqueta introducida.
Etiquetado de conmutador invitado (VGT)	4095	Las máquinas virtuales controlan las VLAN. El conmutador virtual transmite tráfico desde cualquier VLAN.

8 En la página Seguridad, anule la configuración del conmutador para la protección contra la suplantación de direcciones MAC y para la ejecución de las máquinas virtuales en modo promiscuo.

9 En la página Catalogación de tráfico, en el nivel de grupo de puertos, anule el tamaño de ancho de banda promedio y pico, y el tamaño de las ráfagas.

10 En la página Formación de equipos y conmutación por error, anule la configuración de formación de equipos y conmutación por error heredada del conmutador estándar.

Puede configurar la distribución del tráfico y el reenrutamiento entre los adaptadores físicos asociados con el grupo de puertos. También puede cambiar el orden en que se utilizan los adaptadores físicos del host en caso de error.

11 Haga clic en **Aceptar**.

Quitar un grupo de puertos desde vSphere Standard Switch

Puede quitar grupos de puertos de vSphere Standard Switch si ya no necesita las redes etiquetadas asociadas.

Requisitos previos

Compruebe que no haya máquinas virtuales encendidas conectadas al grupo de puertos que desea quitar.

Procedimiento

1 En vSphere Web Client, desplácese hasta el host.

2 En la pestaña **Configurar**, expanda **Redes** y seleccione **Conmutadores virtuales**.

3 Seleccione el conmutador estándar.

4 En el diagrama de topología del conmutador, haga clic en la etiqueta del grupo de puertos que desea quitar para seleccionarlo.

5 En la barra de herramientas de la topología del conmutador, haga clic en el icono de acción **Quitar grupo de puertos seleccionado**.

Propiedades de vSphere Standard Switch

La configuración de vSphere Standard Switch controla en todo el conmutador los valores predeterminados de los puertos, a los cuales la configuración del grupo de puertos correspondiente a cada conmutador estándar puede ignorar. Es posible editar las propiedades del conmutador estándar, como la configuración de vínculo superior y la cantidad de puertos disponibles.

Cantidad de puertos en los hosts ESXi

Para asegurar un uso eficiente de los recursos en los hosts que ejecutan ESXi 5.5 y versiones posteriores, los puertos de conmutadores virtuales se escalan dinámicamente de forma vertical y horizontal. Un conmutador en dicho host puede expandirse hasta la cantidad máxima de puertos admitidos en el host. El límite de puertos se determina en función de la cantidad máxima de máquinas virtuales que el host puede manejar.

Cada conmutador virtual en los hosts que ejecutan ESXi 5.1 y versiones anteriores proporciona una cantidad finita de puertos a través de los cuales las máquinas virtuales y los servicios de red pueden alcanzar una o más redes. Es necesario aumentar o disminuir manualmente la cantidad de puertos de acuerdo con sus requisitos de implementación.

Nota El aumento de la cantidad de puertos de un conmutador hará que se reserven y se consuman más recursos en el host. Si algunos puertos no estuvieran ocupados, los recursos del host que podrían ser necesarios para otras operaciones permanecerán bloqueados y sin usar.

Cambiar tamaño de la MTU en vSphere Standard Switch

Cambie el tamaño de la unidad de transmisión máxima (MTU) en vSphere Standard Switch para mejorar la eficacia de las redes gracias al aumento de los datos de carga útil que se transmite en un paquete, es decir, habilitando las tramas gigantes.

Procedimiento

1 En vSphere Web Client, desplácese hasta el host.

2 En la pestaña **Configurar**, expanda **Redes** y seleccione **Conmutadores virtuales**.

3 Seleccione un conmutador estándar de la tabla y haga clic en **Editar configuración**.

4 Cambie el valor de **MTU (bytes)** para el conmutador estándar.

   Para habilitar tramas gigantes, configure un valor de MTU superior a 1.500. El valor máximo para el tamaño de MTU es de 9.000 bytes.

5 Haga clic en **Aceptar**.

Cambiar la velocidad de un adaptador físico

Un adaptador físico puede representar un cuello de botella para el tráfico de red si la velocidad del adaptador no coincide con los requisitos de las aplicaciones. Puede modificar la velocidad de conexión y dúplex de un adaptador físico para transmitir datos de acuerdo con la velocidad de tráfico.

Si el adaptador físico admite SR-IOV, puede habilitarlo y configurar la cantidad de funciones virtuales que se utilizarán para las redes de máquinas virtuales.

Procedimiento

1 En vSphere Web Client, desplácese hasta un host.

2 En la pestaña **Configurar**, expanda **Redes** y seleccione **Adaptadores físicos**.

   Los adaptadores de red físicos del host se muestran en una tabla que contiene detalles de cada adaptador de red físico.

3 Seleccione el adaptador de red físico en la lista y haga clic en el icono **Editar la configuración del adaptador**.

4 Seleccione la velocidad y el modo dúplex del adaptador de red físico en el menú desplegable.

5 Haga clic en **Aceptar**.

Agregar y agrupar adaptadores físicos en vSphere Standard Switch

Asigne un adaptador físico a un conmutador estándar para brindar conectividad a las máquinas virtuales y los adaptadores VMkernel del host. Puede formar un equipo de NIC para distribuir la carga del tráfico y configurar la conmutación por error.

La formación de equipos de NIC combina varias conexiones de red para aumentar la capacidad de proceso y ofrecer redundancia si un vínculo presenta errores. Para crear un equipo, se asocian varios adaptadores físicos a vSphere Standard Switch.

Procedimiento

1 En vSphere Web Client, desplácese hasta el host.

2 En la pestaña **Configurar**, expanda **Redes** y seleccione **Conmutadores virtuales**.

3 Seleccione el conmutador estándar al que desea agregar un adaptador físico.

4 Haga clic en el icono **Administrar los adaptadores de redes físicas conectados al conmutador seleccionado**.

5 Agregue uno o varios adaptadores de red físicos disponibles al conmutador.

   a Haga clic en **Agregar adaptadores**.

   b Seleccione el grupo de orden de conmutación por error al cual se deben asignar los adaptadores.

      El grupo de conmutación por error determina el rol del adaptador en el intercambio de datos con la red externa; ese rol puede ser activo, en espera o sin usar. De forma predeterminada, los adaptadores se agregan al conmutador estándar en modo activo.

   c Haga clic en **Aceptar**.

   Los adaptadores seleccionados aparecen en la lista del grupo de conmutación por error seleccionado, bajo la lista Adaptadores asignados.

6 (opcional) Use las flechas hacia arriba y hacia abajo para cambiar la posición de un adaptador dentro del grupo de conmutación por error.

7 Haga clic en **Aceptar** para aplicar la configuración del adaptador físico.

Ver el diagrama de topología de vSphere Standard Switch

El diagrama de topología permite examinar la estructura y los componentes de vSphere Standard Switch.

El diagrama de topología de un conmutador estándar ofrece una representación visual de los adaptadores y los grupos de puertos conectados al conmutador.

Desde el diagrama, es posible editar la configuración de un grupo de puertos seleccionado y de un adaptador seleccionado.

Procedimiento

1 En vSphere Web Client, desplácese hasta el host.

2 En la pestaña **Configurar**, expanda **Redes** y seleccione **Conmutadores virtuales**.

3 Seleccione el conmutador estándar en la lista.

Resultados

El diagrama aparece debajo de la lista de conmutadores virtuales del host.

Ejemplo: Diagrama de un conmutador estándar que conecta el VMkernel y las máquinas virtuales a la red

En el entorno virtual, vSphere Standard Switch controla los adaptadores VMkernel para vSphere vMotion y para la red de administración, y las máquinas virtuales agrupadas. Es posible utilizar el diagrama de topología central para examinar si una máquina virtual o un adaptador VMkernel están conectados a la red externa y para identificar el adaptador físico que transporta los datos.

Figura 2-2. Diagrama de topología de un conmutador estándar que conecta el VMkernel y las máquinas virtuales a la red



Configurar redes con conmutadores distribuidos de vSphere

3

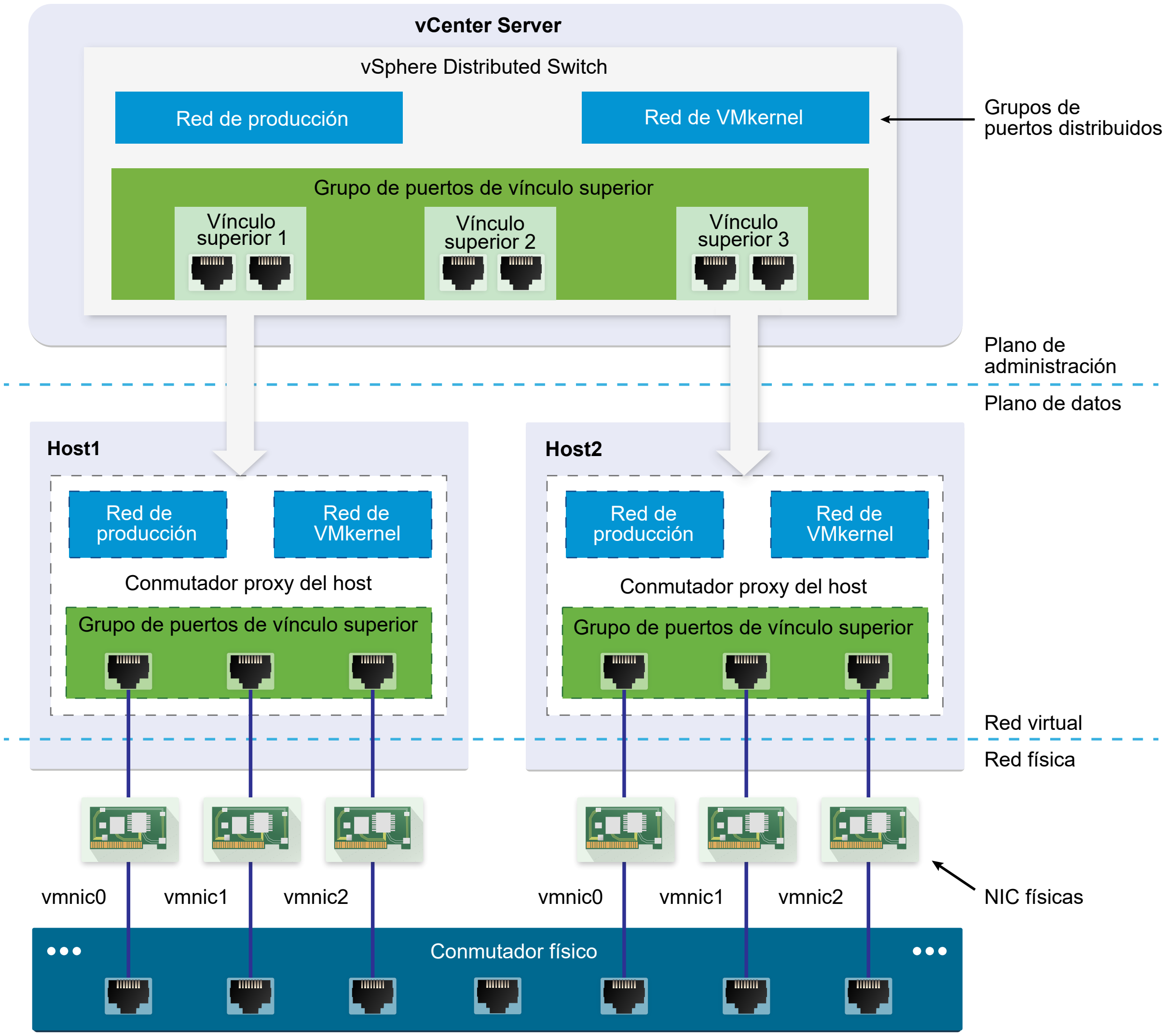
Con los conmutadores distribuidos de vSphere, se pueden instalar y configurar redes en un entorno de vSphere.

Este capítulo incluye los siguientes temas:

Arquitectura de vSphere Distributed Switch

vSphere Distributed Switch ofrece administración y supervisión centralizada de la configuración de redes de todos los hosts asociados con el conmutador. El conmutador distribuido se establece en un sistema vCenter Server y sus opciones de configuración se propagan a todos los hosts asociados con el conmutador.

Figura 3-1. Arquitectura de vSphere Distributed Switch



El conmutador de red en vSphere consta de dos secciones lógicas: el plano de datos y el plano de administración. El plano de datos implementa la conmutación, el filtrado y el etiquetado de paquetes, entre otras funciones. El plano de administración es la estructura de control que se utiliza para configurar la funcionalidad del plano de datos. vSphere Standard Switch contiene los planos de datos y de administración, y cada conmutador estándar se configura y se mantiene de forma individual.

vSphere Distributed Switch separa el plano de datos del plano de administración. La funcionalidad de administración del conmutador distribuido reside en el sistema vCenter Server que permite administrar la configuración de redes del entorno en el nivel del centro de datos. El plano de datos se conserva de forma local en cada host asociado con el conmutador distribuido. La sección del plano de datos del conmutador distribuido se denomina conmutador proxy del host. La configuración de redes que se crea en vCenter Server (el plano de administración) se transmite automáticamente a todos los conmutadores proxy del host (el plano de datos).

vSphere Distributed Switch incorpora dos abstracciones que se utilizan para crear una configuración de redes uniforme para las NIC físicas, las máquinas virtuales y los servicios VMkernel.

Grupo de puertos de vínculo superior

Un grupo de puertos de vínculo superior o de dvuplink se define durante la creación del conmutador distribuido, y puede tener uno o varios vínculos superiores. Un vínculo superior es una plantilla que se utiliza para configurar las conexiones físicas de los hosts y las directivas de conmutación por error y equilibrio de carga. Las NIC físicas de los hosts se asignan a los vínculos superiores en el conmutador distribuido. En el nivel del host, cada NIC física está conectada a un puerto de vínculo superior con un identificador particular. Las directivas de conmutación por error y equilibrio de carga se establecen a través de los vínculos superiores y se propagan automáticamente a los conmutadores proxy del plano de datos. De esta forma, es posible aplicar una configuración uniforme de conmutación por error y equilibrio de carga para las NIC físicas de todos los hosts asociados con el conmutador distribuido.

Grupo de puertos distribuidos

Los grupos de puertos distribuidos ofrecen conectividad de red a las máquinas virtuales y admiten el tráfico VMkernel. Para identificar cada grupo de puertos distribuidos, se utiliza una etiqueta de red que debe ser exclusiva del centro de datos actual. Es posible configurar directivas de formación de equipos de NIC, conmutación por error, equilibrio de carga, VLAN, seguridad, catalogación de tráfico y otras directivas en los grupos de puertos. Los puertos virtuales conectados a un grupo de puertos distribuidos comparten las mismas propiedades que se configuran para el grupo de puertos distribuidos. Tal como ocurre con los grupos de puertos de vínculo superior, la configuración que se establece en los grupos de puertos distribuidos en vCenter Server (el plano de administración) se propaga automáticamente a todos los hosts del conmutador distribuido a través de los conmutadores proxy del host (el plano de datos). De esta forma, es posible configurar un grupo de máquinas virtuales para que compartan la misma configuración de redes si se asocian las máquinas virtuales al mismo grupo de puertos distribuidos.

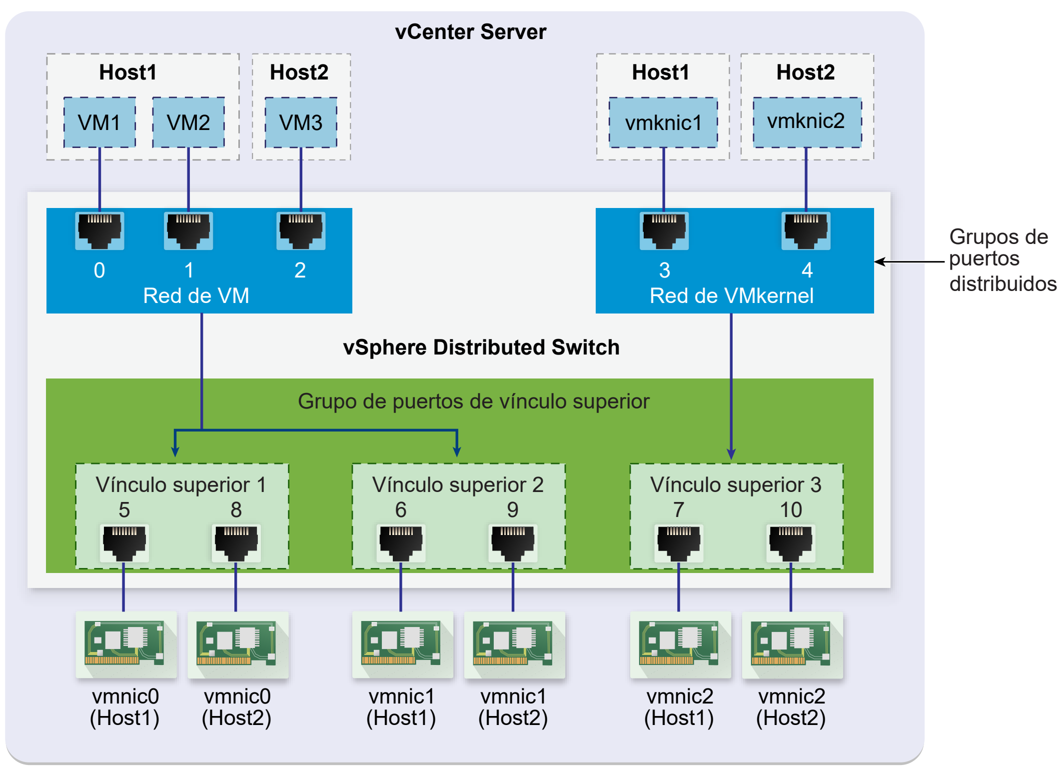
Por ejemplo, suponga que crea un vSphere Distributed Switch en el centro de datos y asocia dos hosts con él. Configura tres vínculos superiores al grupo de puertos de vínculo superior y conecta la NIC física de cada host al vínculo superior. De esta forma, cada vínculo superior tiene asignadas dos NIC físicas de cada host, por ejemplo, el vínculo superior 1 está configurado con vmnic0 desde el host 1 y el host 2. A continuación, crea los grupos de puertos distribuidos de red de producción y VMkernel para los servicios de redes y VMkernel de la máquina virtual. También se crea una representación de los grupos de puertos de red de producción y VMkernel en el host 1 y el host 2, respectivamente. Todas las directivas establecidas en los grupos de puertos de red de producción y VMkernel se propagan a sus representaciones en el host 1 y el host 2.

Para garantizar el uso eficaz de los recursos del host, la cantidad de puertos distribuidos de los conmutadores proxy se incrementa y se reduce dinámicamente en los hosts donde se ejecuta ESXi 5.5 y versiones posteriores. Un conmutador proxy de este tipo de host puede expandirse hasta la cantidad máxima de puertos admitida por el host. El límite de puertos se determina en función de la cantidad máxima de máquinas virtuales que el host puede manejar.

Flujo de datos de vSphere Distributed Switch

El flujo de datos desde las máquinas virtuales y los adaptadores VMkernel hacia la red física depende de las directivas de equilibrio de carga y formación de equipos de NIC que se establecen en los grupos de puertos distribuidos. El flujo de datos también depende de la asignación de puertos en el conmutador distribuido.

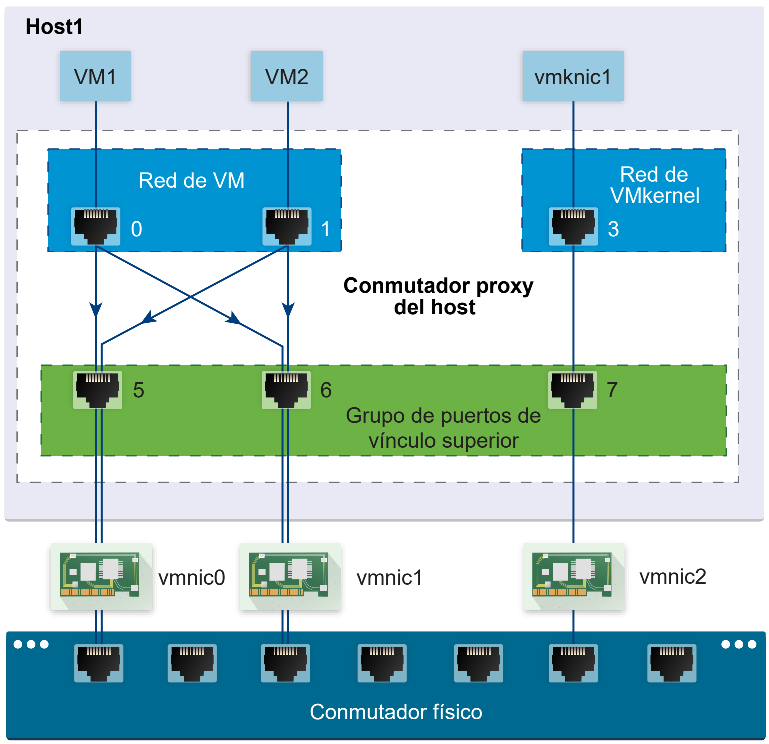
Figura 3-2. Formar equipos de NIC y asignar puertos en vSphere Distributed Switch



Por ejemplo, suponga que crea los grupos de puertos distribuidos de la red de máquina virtual y de la red del VMkernel con 3 y 2 puertos distribuidos, respectivamente. El conmutador distribuido asigna los puertos con los identificadores de 0 a 4 en el orden en que se crearon los grupos de puertos distribuidos. A continuación, se asocian los hosts 1 y 2 con el conmutador distribuido. El conmutador distribuido asigna los puertos de cada NIC física en los hosts, ya que la numeración de los puertos continúa a partir de 5 en el orden en que se agregan los hosts. Para brindar conectividad de red a cada host, debe asignar vmnic0 al vínculo superior 1, vmnic1 al vínculo superior 2 y vmnic2 al vínculo superior 3.

Para brindar conectividad a las máquinas virtuales e incluir el tráfico VMkernel, configure la formación de equipos y conmutación por error a la red de máquina virtual y a los grupos de puertos de red del VMkernel. El vínculo superior 1 y el vínculo superior 2 controlan el tráfico del grupo de puertos de red de máquina virtual, y el vínculo superior 3 controla el tráfico del grupo de puertos de red del VMkernel.

Figura 3-3. Flujo de paquetes en el conmutador proxy del host



En el host, el flujo de paquetes de las máquinas virtuales y los servicios VMkernel pasa a través de puertos específicos para llegar a la red física. Por ejemplo, un paquete enviado desde VM1 en el host 1 llega primero al puerto 0 del grupo de puertos distribuidos de red de máquina virtual. Como el vínculo superior 1 y el vínculo superior 2 controlan el tráfico del grupo de puertos de red de máquina virtual, el paquete puede continuar desde el puerto de vínculo superior 5 o el puerto de vínculo superior 6. Si el paquete pasa por el puerto de vínculo superior 5, sigue hasta vmnic0, y si el paquete pasa por el puerto de vínculo superior 6, sigue hasta vmnic1.

Crear vSphere Distributed Switch

Cree un conmutador distribuido de vSphere en un centro de datos para controlar la configuración de redes de varios hosts al mismo tiempo desde un punto central.

Procedimiento

1 En vSphere Web Client, desplácese hasta un centro de datos.

2 En el navegador, haga clic con el botón derecho en el centro de datos y seleccione **Conmutador distribuido > Nuevo conmutador distribuido**.

3 En la página Nombre y ubicación, escriba un nombre para el nuevo conmutador distribuido o acepte el nombre generado y, a continuación, haga clic en**Siguiente**.

4 En la página Seleccionar versión, seleccione la versión del conmutador distribuido y haga clic en **Siguiente**.

Opción	Descripción
Distributed Switch: 6.5.0	Compatible con ESXi 6.5 y versiones posteriores.
Distributed Switch: 6.0.0	Compatible con ESXi 6.0 y versiones posteriores. No se admiten características presentes en las versiones posteriores de vSphere Distributed Switch.
Distributed Switch: 5.5.0	Compatible con ESXi 5.5 y versiones posteriores. No se admiten características presentes en las versiones posteriores de vSphere Distributed Switch.
Distributed Switch: 5.1.0	Compatible con VMware ESXi 5.1 y versiones posteriores. No se admiten características presentes en las versiones posteriores de vSphere Distributed Switch.
Distributed Switch: 5.0.0	Compatible con VMware ESXi 5.0 y versiones posteriores. No se admiten características presentes en las versiones posteriores de vSphere Distributed Switch.

5 En la página Editar configuración, configure las opciones del conmutador distribuido.

a Utilice los botones de flecha para seleccionar un valor de **Cantidad de vínculos superiores**.

Los puertos de vínculo superior conectan el conmutador distribuido a las NIC físicas en los hosts asociados. La cantidad de puertos de vínculo superior es la cantidad de conexiones físicas permitidas con el conmutador distribuido por host.

b Utilice el menú desplegable para habilitar o deshabilitar **Network I/O Control**.

Network I/O Control permite priorizar el acceso a los recursos de red para ciertos tipos de infraestructura y tráfico de carga de trabajo en función de los requisitos de su implementación. Network I/O Control supervisa continuamente la carga de E/S a través de la red y asigna los recursos disponibles de forma dinámica.

c Active la casilla **Crear un grupo de puertos predeterminado** para crear un nuevo grupo de puertos distribuidos con la configuración predeterminada de este conmutador.

d (opcional) Para crear un grupo de puertos distribuidos predeterminado, escriba el nombre del grupo de puertos en el campo **Nombre del grupo de puertos** o acepte el nombre generado.

Si el sistema tiene requisitos personalizados para el grupo de puertos, cree grupos de puertos distribuidos que cumplan esos requisitos después de agregar el conmutador distribuido.

e Haga clic en **Siguiente**.

6 En la página Listo para finalizar, revise la nueva configuración seleccionada y haga clic en **Finalizar**.

   Utilice el botón **Atrás** para editar cualquier configuración.

Resultados

Se crea un conmutador distribuido en el centro de datos. Puede ver las características admitidas en el conmutador distribuido, así como otros detalles, si se desplaza hasta el nuevo conmutador distribuido y hace clic en la pestaña **Resumen**.

Pasos siguientes

Agregue hosts al conmutador distribuido y configure los adaptadores de red en el conmutador.

Actualizar vSphere Distributed Switch a una versión posterior

Es posible actualizar vSphere Distributed Switch versión 5.x a una versión posterior. La actualización permite que el conmutador distribuido aproveche las características que solo están disponibles en la versión posterior.

La actualización de un conmutador distribuido es una operación sin interrupciones; es decir, los hosts y las máquinas virtuales asociados al conmutador no experimentan ningún tiempo de inactividad.

Nota Para poder restaurar la conectividad de las máquinas virtuales y los adaptadores VMkernel si la actualización presenta errores, haga una copia de seguridad de la configuración del conmutador distribuido.

Si la actualización no se realiza correctamente, para recrear el conmutador con sus grupos de puertos y hosts conectados, puede importar el archivo de configuración del conmutador. Consulte Exportar la configuración de vSphere Distributed Switch y Importar la configuración de vSphere Distributed Switch.

Requisitos previos

- Actualice vCenter Server a la versión 6.5.
- Actualice todos los hosts conectados al conmutador distribuido a ESXi 6.5.

Procedimiento

1 En vSphere Web Client, desplácese hasta el conmutador distribuido.

2 Haga clic con el botón derecho en el conmutador distribuido y seleccione **Actualizar > Actualizar conmutador distribuido**.

3 Seleccione la versión de vSphere Distributed Switch a la que desea actualizar el conmutador y haga clic en **Siguiente**.

Opción	Descripción
Versión 6.5.0	Compatible con ESXi versión 6.5 y posteriores.
Versión 6.0.0	Compatible con ESXi versión 6.0 y posteriores. No se admiten características presentes en las versiones posteriores de vSphere Distributed Switch.
Versión 5.5.0	Compatible con ESXi versión 5.5 y posteriores. No se admiten características presentes en las versiones posteriores de vSphere Distributed Switch.
Versión 5.1.0	Compatible con ESXi versión 5.1 y posteriores. No se admiten características presentes en las versiones posteriores de vSphere Distributed Switch.

4 Revise la compatibilidad de host y haga clic en **Siguiente**.

Algunos casos de ESXi que están conectados al conmutador distribuido pueden ser incompatibles con la versión de destino seleccionada. Actualice o quite los hosts no compatibles, o bien seleccione otra versión de actualización para el conmutador distribuido.

5 Complete la configuración de actualización y haga clic en **Finalizar**.

Precaución Después de actualizar vSphere Distributed Switch no es posible volver a una versión anterior. Tampoco se pueden agregar hosts ESXi que ejecutan una versión anterior a la nueva versión del conmutador.

a Revise la configuración de actualización.

b Si actualiza desde vSphere Distributed Switch 5.1, programe la conversión a la compatibilidad con LACP mejorada.

c Si actualiza desde vSphere Distributed Switch 5.1 y posterior, programe la conversión a la versión 3 de Network I/O Control.

Resultados

Para obtener información sobre cómo convertir a la compatibilidad con LACP mejorada, consulte Convertir la compatibilidad con LACP mejorada en vSphere Distributed Switch.

Para obtener información sobre cómo convertir a la versión 3 de Network I/O Control, consulte Actualizar Network I/O Control a la versión 3 en vSphere Distributed Switch .

Editar la configuración general y avanzada de vSphere Distributed Switch

Las opciones de la configuración general de vSphere Distributed Switch incluyen el nombre del conmutador y la cantidad de vínculos superiores. La configuración avanzada para un conmutador distribuido incluye el protocolo Cisco Discovery Protocol y el valor de MTU máximo para el conmutador.

Procedimiento

1 En vSphere Web Client, desplácese hasta el conmutador distribuido.

2 En la pestaña **Configurar**, expanda **Configuración** y seleccione **Propiedades**.

3 Haga clic en **Editar**.

4 Haga clic en **Configuración general** para editar la configuración de vSphere Distributed Switch.

Opción	Descripción
Nombre	Escriba el nombre del conmutador distribuido.
Cantidad de vínculos superiores	Seleccione la cantidad de puertos de vínculo superior para el conmutador distribuido. Haga clic en **Editar nombres de vínculos superiores** para modificar los nombres de los vínculos superiores.
Cantidad de puertos	La cantidad de puertos del conmutador distribuido. No es posible editar este valor.
Network I/O Control	Use el menú desplegable para habilitar o deshabilitar Network I/O Control.
Descripción	Agregue o modifique una descripción de la configuración del conmutador distribuido.

5 Haga clic en **Configuración avanzada** para editar la configuración de vSphere Distributed Switch.

Opción	Descripción
MTU (Bytes)	Tamaño máximo de MTU para vSphere Distributed Switch. Para habilitar las tramas gigantes, establezca un valor superior a 1.500.
Modo de filtrado multidifusión	■ **Básico**. El conmutador distribuido reenvía el tráfico relacionado con un grupo multidifusión en función de una dirección MAC generada a partir de los últimos 23 bits de la dirección IPv4 del grupo. ■ **Intromisión IGMP/MLD**. El conmutador distribuido reenvía el tráfico multidifusión a las máquinas virtuales en función de las direcciones IPv4 e IPv6 de los grupos de multidifusión suscritos mediante mensajes de pertenencia definidos por el protocolo Internet Group Management Protocol (IGMP) y el protocolo Multicast Listener Discovery.
Protocolo de detección	a Seleccione Cisco Discovery Protocol, Link Layer Discovery Protocol o Deshabilitado en el menú desplegable **Tipo**. b Establezca la opción Operación en Escuchar, Anunciar o Ambas. Para obtener información sobre el protocolo de detección, consulte Protocolo de detección de conmutadores.
Contacto del administrador	Escriba el nombre y otros detalles del administrador del conmutador distribuido.

6 Haga clic en **Aceptar**.

Administrar redes en varios hosts en vSphere Distributed Switch

Para crear y administrar redes virtuales en vSphere Distributed Switch, agregue hosts al conmutador y conecte los adaptadores de red al conmutador. Si desea crear una configuración de redes uniforme para varios hosts del conmutador distribuido, puede usar un host como plantilla y aplicar su configuración a los demás hosts.

- Tareas para administrar redes de host en vSphere Distributed Switch

  Se pueden agregar nuevos hosts a vSphere Distributed Switch, conectar adaptadores de red al conmutador y quitar los hosts del conmutador. En un entorno de producción, es posible que se deba mantener la conectividad de red de las máquinas virtuales y los servicios de VMkernel mientras se administran las redes del host del conmutador distribuido.

- Agregar hosts a vSphere Distributed Switch

  Para administrar las redes del entorno de vSphere mediante vSphere Distributed Switch, debe asociar los hosts con el conmutador. Para ello, conecte las NIC físicas, los adaptadores VMkernel y los adaptadores de red de las máquinas virtuales de los hosts al conmutador distribuido.

- Configurar adaptadores de red físicos en vSphere Distributed Switch

  Es posible asignar NIC físicas para vínculos superiores en el conmutador a los hosts asociados con un conmutador distribuido. Se pueden configurar NIC físicas en el conmutador distribuido para varios hosts a la vez.

- Migrar adaptadores VMkernel a vSphere Distributed Switch

  Migre los adaptadores VMkernel a un conmutador distribuido si desea controlar el tráfico correspondiente a los servicios VMkernel utilizando solo este conmutador, y ya no necesitará los adaptadores en otros conmutadores distribuidos o estándar.

- Crear un adaptador VMkernel en vSphere Distributed Switch

  Cree un adaptador VMkernel en hosts asociados con un conmutador distribuido para proporcionar conectividad de red a los hosts y para manejar el tráfico de vSphere vMotion, almacenamiento IP, registro de Fault Tolerance y vSAN. Puede crear adaptadores VMkernel en varios hosts de manera simultánea utilizando el asistente **Agregar y administrar hosts**.

- Migrar redes de máquinas virtuales a vSphere Distributed Switch

  Para administrar redes de máquinas virtuales mediante un conmutador distribuido, migre los adaptadores de redes de máquinas virtuales a las redes etiquetadas en el conmutador.

- Utilizar un host como plantilla para crear una configuración de redes uniforme en vSphere Distributed Switch

  Si planifica incluir hosts con una configuración de redes uniforme, puede seleccionar un host como plantilla y aplicar su configuración para las NIC físicas y los adaptadores VMkernel a otros host del conmutador distribuido.

- Quitar hosts de vSphere Distributed Switch

  Quite los hosts de un conmutador distribuido de vSphere si configuró un conmutador diferente para los hosts.

Tareas para administrar redes de host en vSphere Distributed Switch

Se pueden agregar nuevos hosts a vSphere Distributed Switch, conectar adaptadores de red al conmutador y quitar los hosts del conmutador. En un entorno de producción, es posible que se deba mantener la conectividad de red de las máquinas virtuales y los servicios de VMkernel mientras se administran las redes del host del conmutador distribuido.

Agregar hosts a vSphere Distributed Switch

Considere preparar el entorno antes de agregar nuevos hosts a un conmutador distribuido.

- Cree grupos de puertos distribuidos para las redes de máquinas virtuales.
- Cree grupos de puertos distribuidos para servicios de VMkernel. Por ejemplo, cree grupos de puertos distribuidos para la red de administración, vMotion y Fault Tolerance.
- Configure suficientes vínculos superiores en el conmutador distribuido para todas las NIC físicas que desea conectar al conmutador. Por ejemplo, si cada host que desea conectar al conmutador distribuido tiene ocho NIC físicas, configure ocho vínculos superiores en el conmutador distribuido.
- Asegúrese de que la configuración del conmutador distribuido esté preparada para los servicios con requisitos de redes específicos. Por ejemplo, iSCSI tiene requisitos específicos para la configuración de formación de equipos y conmutación por error del grupo de puertos distribuidos donde se conecta el adaptador VMkernel de iSCSI.

Se puede utilizar el asistente **Agregar y administrar hosts** en vSphere Web Client para agregar varios hosts a la vez.

Administrar adaptadores de red en vSphere Distributed Switch

Después de agregar los hosts a un conmutador distribuido, se pueden conectar NIC físicas a los vínculos superiores del conmutador, configurar adaptadores de red de las máquinas virtuales y administrar las redes VMkernel.

Si algunos hosts de un conmutador distribuido están asociados a otros conmutadores del centro de datos, se pueden migrar los adaptadores de red hacia o desde el conmutador distribuido.

Si se migran adaptadores de red de la máquina virtual o adaptadores VMkernel, asegúrese de que los grupos de puertos distribuidos de destino tengan al menos un vínculo superior activo y que este esté conectado a una NIC física en los hosts. Otro método es migrar las NIC físicas, los adaptadores de red virtuales y los adaptadores VMkernel simultáneamente.

Si se migran las NIC físicas, deje al menos una NIC activa que controle el tráfico de los grupos de puertos. Por ejemplo, si *vmnic0* y *vmnic1* controlan el tráfico del grupo de puertos *VM Network*, migre *vmnic0* y deje *vmnic1* conectada al grupo.

Quitar hosts de vSphere Distributed Switch

Antes de quitar hosts de un conmutador distribuido, debe migrar los adaptadores de red que están en uso a otro conmutador.

- Para agregar hosts a un conmutador distribuido diferente, se puede utilizar el asistente **Agregar y administrar hosts** a fin de migrar en bloque los adaptadores de red de los hosts al nuevo conmutador. A continuación, se pueden extraer los hosts de forma segura de su conmutador distribuido actual.
- Para migrar las redes del host a conmutadores estándar, se deben migrar los adaptadores de red por etapas. Por ejemplo, quite las NIC físicas en los hosts del conmutador distribuido; para ello, deje una NIC física en cada host conectada al conmutador para mantener la conectividad de red. A continuación, asocie las NIC físicas a los conmutadores estándar y migre los adaptadores VMkernel y los adaptadores de red de la máquina virtual a los conmutadores. Por último, migre la NIC física que dejó conectada al conmutador distribuido a los conmutadores estándar.

Agregar hosts a vSphere Distributed Switch

Para administrar las redes del entorno de vSphere mediante vSphere Distributed Switch, debe asociar los hosts con el conmutador. Para ello, conecte las NIC físicas, los adaptadores VMkernel y los adaptadores de red de las máquinas virtuales de los hosts al conmutador distribuido.

Requisitos previos

- Compruebe que haya suficientes vínculos superiores disponibles en el conmutador distribuido para asignarles las NIC físicas que desea conectar al conmutador.
- Compruebe que haya al menos un grupo de puertos distribuidos en el conmutador distribuido.
- Compruebe que el grupo de puertos distribuidos tenga configurados vínculos superiores activos en su directiva de formación de equipos y conmutación por error.

Si migra o crea adaptadores VMkernel para iSCSI, compruebe que la directiva de formación de equipos y conmutación por error del grupo de puertos distribuidos de destino cumpla con los requisitos de iSCSI:

- Compruebe que haya activo un solo vínculo superior, que la lista en espera esté vacía y que el resto de los vínculos superiores estén sin utilizar.
- Compruebe que se haya asignado una sola NIC física por host al vínculo superior activo.

Procedimiento

1 En vSphere Web Client, desplácese hasta el conmutador distribuido.

2 En el menú **Acciones**, seleccione **Agregar y administrar hosts**.

3 En la página Seleccionar tarea, seleccione **Agregar hosts** y haga clic en **Siguiente**.

4 En la página Seleccionar hosts, haga clic en **Nuevos hosts**, seleccione uno de los hosts del centro de datos y haga clic en **Aceptar** y, a continuación, haga clic en **Siguiente**.

5 En la página Seleccionar tareas del adaptador de red, seleccione las tareas para configurar adaptadores de red en el conmutador distribuido y haga clic en **Siguiente**.

6 En la página Administrar adaptadores de red físicos, configure las NIC físicas en el conmutador distribuido.

   a En la lista En otros conmutadores/sin reclamar, seleccione una NIC física.

      Si selecciona NIC físicas que ya están conectadas a otros conmutadores, estas se migrarán al conmutador distribuido actual.

   b Haga clic en **Asignar vínculo superior**.

   c Seleccione un vínculo superior y haga clic en **Aceptar**.

   Para obtener una configuración de red coherente, se puede conectar una misma NIC física en cada host al mismo vínculo superior en el conmutador distribuido.

   Por ejemplo, si se agregan dos hosts, conecte *vmnic1* en cada host al vínculo *Uplink1* del conmutador distribuido.

7 Haga clic en **Siguiente**.

8 En la página Administrar adaptadores de red de VMkernel, configure los adaptadores de VMkernel.

   a Seleccione un adaptador VMkernel y haga clic en **Asignar grupo de puertos**.

   b Seleccione un grupo de puertos distribuidos y haga clic en **Aceptar**.

9 Revise los servicios afectados y también el nivel de impacto.

Opción	Descripción
Sin impacto	iSCSI continuará con su funcionamiento normal después de aplicar la nueva configuración de redes.
Impacto importante	El funcionamiento normal de iSCSI podría interrumpirse si se aplica la nueva configuración de redes.
Impacto crítico	El funcionamiento normal de iSCSI se verá interrumpido si se aplica la nueva configuración de redes.

   a Si el impacto en iSCSI es importante o crítico, haga clic en la entrada **iSCSI** y revise los motivos que aparecen en el panel de detalles Análisis.

   b Después de solucionar el problema del impacto en iSCSI, continúe con su configuración de redes.

10 Haga clic en **Siguiente**.

11 En la página Migrar redes de máquina virtual, configure las redes de la máquina virtual.

   a Para conectar todos los adaptadores de red de una máquina virtual a un grupo de puertos distribuido, seleccione la máquina virtual o seleccione un adaptador de red individual para conectar solamente el adaptador.

   b Haga clic en **Asignar grupo de puertos**.

   c Seleccione un grupo de puertos distribuidos de la lista y haga clic en **Aceptar**.

12 Haga clic en **Siguiente** y, a continuación, en **Finalizar**.

Pasos siguientes

Al tener hosts asociados con el conmutador distribuido, se pueden administrar NIC físicas, adaptadores VMkernel y adaptadores de red de las máquinas virtuales.

Configurar adaptadores de red físicos en vSphere Distributed Switch

Es posible asignar NIC físicas para vínculos superiores en el conmutador a los hosts asociados con un conmutador distribuido. Se pueden configurar NIC físicas en el conmutador distribuido para varios hosts a la vez.

Para obtener una configuración de redes coherente en todos los hosts, es posible asignar la misma NIC física en cada host al mismo vínculo superior en el conmutador distribuido. Por ejemplo, se puede asignar *vmnic1* de los hosts *ESXi A* y *ESXi B* a *Uplink 1*.

Procedimiento

1 En vSphere Web Client, desplácese hasta el conmutador distribuido.

2 En el menú **Acciones**, seleccione **Agregar y administrar hosts**.

3 En **Seleccionar tarea**, seleccione **Administrar red de host** y haga clic en **Siguiente**.

4 En **Seleccionar hosts**,haga clic en **Hosts conectados** y seleccione entre los hosts que están asociados con el conmutador distribuido.

5 Haga clic en **Siguiente**.

6 En **Seleccionar tareas del adaptador de red**, seleccione **Administrar adaptadores físicos** y haga clic en **Siguiente**.

7 En **Administrar adaptadores de red físicos**, seleccione una NIC física de la lista En otros conmutadores/sin reclamar.

   Si selecciona NIC físicas que ya se asignaron a otros conmutadores, estas se migrarán al conmutador distribuido actual.

8 Haga clic en **Asignar vínculo superior**.

9 Seleccione un vínculo superior o seleccione **Asignación automática**.

10 Haga clic en **Siguiente**.

11 Revise los servicios afectados y también el nivel de impacto.

Opción	Descripción
Sin impacto	iSCSI continuará con su funcionamiento normal después de aplicar la nueva configuración de redes.
Impacto importante	El funcionamiento normal de iSCSI podría interrumpirse si se aplica la nueva configuración de redes.
Impacto crítico	El funcionamiento normal de iSCSI se verá interrumpido si se aplica la nueva configuración de redes.

a Si el impacto en iSCSI es importante o crítico, haga clic en la entrada **iSCSI** y revise los motivos que aparecen en el panel de detalles Análisis.

b Después de solucionar el problema del impacto en iSCSI, continúe con su configuración de redes.

12 Haga clic en **Siguiente** y, a continuación, en **Finalizar**.

Migrar adaptadores VMkernel a vSphere Distributed Switch

Migre los adaptadores VMkernel a un conmutador distribuido si desea controlar el tráfico correspondiente a los servicios VMkernel utilizando solo este conmutador, y ya no necesitará los adaptadores en otros conmutadores distribuidos o estándar.

Procedimiento

1 En vSphere Web Client, desplácese hasta el conmutador distribuido.

2 En el menú **Acciones**, seleccione **Agregar y administrar hosts**.

3 En **Seleccionar tarea**, seleccione **Administrar red de host** y haga clic en **Siguiente**.

4 En **Seleccionar hosts**,haga clic en **Hosts conectados** y seleccione entre los hosts que están asociados con el conmutador distribuido.

5 Haga clic en **Siguiente**.

6 En **Seleccionar tareas del adaptador de red**, seleccione **Administrar adaptadores de VMkernel** y haga clic en **Siguiente**.

7 En **Administrar adaptadores de VMkernel**, seleccione el adaptador y haga clic en **Asignar grupo de puertos**.

8 Seleccione un grupo de puertos distribuidos y haga clic en **Aceptar**.

9 Haga clic en **Siguiente**.

10 Revise los servicios afectados y también el nivel de impacto.

Opción	Descripción
Sin impacto	iSCSI continuará con su funcionamiento normal después de aplicar la nueva configuración de redes.
Impacto importante	El funcionamiento normal de iSCSI podría interrumpirse si se aplica la nueva configuración de redes.
Impacto crítico	El funcionamiento normal de iSCSI se verá interrumpido si se aplica la nueva configuración de redes.

a Si el impacto en iSCSI es importante o crítico, haga clic en la entrada **iSCSI** y revise los motivos que aparecen en el panel de detalles Análisis.

b Después de solucionar el problema del impacto en iSCSI, continúe con su configuración de redes.

11 Haga clic en **Siguiente** y, a continuación, en **Finalizar**.

Crear un adaptador VMkernel en vSphere Distributed Switch

Cree un adaptador VMkernel en hosts asociados con un conmutador distribuido para proporcionar conectividad de red a los hosts y para manejar el tráfico de vSphere vMotion, almacenamiento IP, registro de Fault Tolerance y vSAN. Puede crear adaptadores VMkernel en varios hosts de manera simultánea utilizando el asistente **Agregar y administrar hosts**.

Debe dedicar un grupo de puertos distribuidos para cada adaptador VMkernel. Cada adaptador VMkernel debe manejar un solo tipo de tráfico.

Procedimiento

1 En vSphere Web Client, desplácese hasta el conmutador distribuido.

2 En el menú **Acciones**, seleccione **Agregar y administrar hosts**.

3 En **Seleccionar tarea**, seleccione **Administrar red de host** y haga clic en **Siguiente**.

4 En **Seleccionar hosts**,haga clic en **Hosts conectados** y seleccione entre los hosts que están asociados con el conmutador distribuido.

5 Haga clic en **Siguiente**.

6 En **Seleccionar tareas del adaptador de red**, seleccione **Administrar adaptadores de VMkernel** y haga clic en **Siguiente**.

7 Haga clic en **Nuevo adaptador**.

Se abre el asistente **Agregar redes**.

8 En **Seleccionar dispositivo de destino**, seleccione un grupo de puertos distribuidos y haga clic en **Siguiente**.

9 En la página Propiedades de puerto, establezca la configuración para el adaptador de VMkernel.

Opción	Descripción
Etiqueta de red	La etiqueta de red se hereda de la etiqueta del grupo de puertos distribuidos.
configuración de IP	Seleccione IPv4, IPv6 o ambas. **Nota** La opción IPv6 no aparece en los hosts en los que no se ha habilitado IPv6.
Pila de TCP/IP	Seleccione una pila de TCP/IP de la lista. Una vez que se configura una pila de TCP/IP para el adaptador de VMkernel, no es posible cambiarla posteriormente. Si selecciona la pila de TCP/IP de aprovisionamiento o de vMotion, solamente podrá usar estas pilas para controlar el tráfico de vMotion o de aprovisionamiento en el host. Todos los adaptadores de VMkernel para vMotion en la pila de TCP/IP predeterminada se deshabilitan para las sesiones futuras de vMotion. Si configura la pila de TCP/IP de aprovisionamiento, los adaptadores de VMkernel en la pila de TCP/IP predeterminada se deshabilitan para las operaciones que incluyan tráfico de aprovisionamiento, como una operación de migración de instantáneas, clonación o migración en frío de una máquina virtual.
Habilitación de servicios	Es posible habilitar servicios para la pila de TCP/IP predeterminada en el host. Seleccione una opción entre los servicios disponibles: ■ **Tráfico de vMotion**. Permite al adaptador de VMkernel anunciarse a otro host como la conexión de red mediante la cual se envía el tráfico de vMotion. La migración con vMotion al host seleccionado no es posible si el servicio de vMotion no se ha habilitado para ningún adaptador de VMkernel en la pila de TCP/IP predeterminada, ni tampoco si no hay adaptadores que estén utilizando la pila de TCP/IP de vMotion. ■ **Tráfico de aprovisionamiento**. Controla los datos que se transfieren para una operación de migración de instantáneas, clonación o migración en frío de una máquina virtual. ■ **Tráfico de Fault Tolerance**. Permite registrar Fault Tolerance en el host. Solamente se puede usar un adaptador de VMkernel por host para el tráfico de FT. ■ **Tráfico de administración**. Habilita el tráfico de administración del host y vCenter Server. Normalmente, se crea un adaptador de VMkernel de este tipo para los hosts cuando se instala el software ESXi. Es posible crear otro adaptador de VMkernel para el tráfico de administración en el host con la finalidad de proporcionar redundancia. ■ **Tráfico de vSphere Replication**. Controla los datos de replicación salientes que se envían desde el host ESXi de origen al servidor de vSphere Replication. ■ **Tráfico NFC de vSphere Replication**. Controla los datos de replicación entrantes en el sitio de replicación de destino. ■ **vSAN**. Habilita el tráfico de vSAN en el host. Todos los hosts que forman parte de un clúster de vSAN deben tener un adaptador de VMkernel de este tipo.

10 Si ha seleccionado las pilas TCP/IP de vMotion o Aprovisionamiento, haga clic en **Aceptar** en el cuadro de diálogo de advertencia que aparece.

Si ya se ha iniciado una operación de migración activa, esta se ejecuta correctamente incluso después de que se deshabilitan los adaptadores de VMkernel involucrados en la pila de TCP/IP predeterminada de vMotion. Lo mismo ocurre con las operaciones que incluyen adaptadores de VMkernel en la pila de TCP/IP predeterminada que están configurados para tráfico de aprovisionamiento.

11 (opcional) En la página Configuración de IPv4, seleccione una opción para obtener las direcciones IP.

Opción	Descripción
Obtener configuración de IPv4 automáticamente	Use DHCP para obtener la configuración de IP. Debe haber un servidor DHCP presente en la red.
Usar configuración de IPv4 estática	Escriba la dirección IP de IPv4 y la máscara de subred para el adaptador VMkernel. Las direcciones de servidor DNS y puerta de enlace predeterminada de VMkernel para IPv4 se obtienen de la pila TCP/IP seleccionada. Active la casilla **Anular la puerta de enlace predeterminada para este adaptador** e introduzca una dirección de puerta de enlace, en caso de que desee especificar una puerta de enlace diferente para el adaptador de VMkernel.

12 (opcional) En la página Configuración de IPv6, seleccione una opción para obtener las direcciones IPv6.

Opción	Descripción
Obtener las direcciones IPv6 automáticamente por medio de DHCP	Use DHCP para obtener las direcciones IPv6. Debe haber un servidor DHCPv6 presente en la red.
Obtener las direcciones IPv6 automáticamente por medio del anuncio de enrutador	Use el anuncio de enrutador para obtener las direcciones IPv6. En ESXi 6.5 y versiones posteriores, el anuncio de enrutador está habilitado de manera predeterminada, y se admiten las marcas M y O según RFC 4861.
Direcciones IPv6 estáticas	a Haga clic en **Agregar dirección IPv6** para agregar una nueva dirección IPv6. b Introduzca la dirección IPv6 y la longitud del prefijo de subred, y haga clic en **Aceptar**. c Para cambiar la puerta de enlace predeterminada de VMkernel, haga clic en **Anular la puerta de enlace predeterminada para este adaptador**. La dirección de puerta de enlace predeterminada de VMkernel para IPv6 se obtiene de la pila de TCP/IP seleccionada.

13 Revise las selecciones de configuración en la página Listo para finalizar y haga clic en **Finalizar**.

14 Siga las instrucciones para completar el asistente.

Migrar redes de máquinas virtuales a vSphere Distributed Switch

Para administrar redes de máquinas virtuales mediante un conmutador distribuido, migre los adaptadores de redes de máquinas virtuales a las redes etiquetadas en el conmutador.

Requisitos previos

Compruebe que exista al menos un grupo de puertos distribuidos destinado a las redes de máquinas virtuales en el conmutador distribuido.

Procedimiento

1. En vSphere Web Client, desplácese hasta el conmutador distribuido.
2. En el menú **Acciones**, seleccione **Agregar y administrar hosts**.
3. En **Seleccionar tarea**, seleccione **Administrar red de host** y haga clic en **Siguiente**.
4. En **Seleccionar hosts**,haga clic en **Hosts conectados** y seleccione entre los hosts que están asociados con el conmutador distribuido.
5. Haga clic en **Siguiente**.
6. En **Seleccionar tareas de adaptador de red**, seleccione **Migrar redes de máquinas virtuales** y haga clic en **Siguiente**.
7. Configure los adaptadores de red de máquinas virtuales al conmutador distribuido.
   a. Para conectar todos los adaptadores de red de una máquina virtual a un grupo de puertos distribuido, seleccione la máquina virtual o seleccione un adaptador de red individual para conectar solamente el adaptador.
   b. Haga clic en **Asignar grupo de puertos**.
   c. Seleccione un grupo de puertos distribuidos de la lista y haga clic en **Aceptar**.
8. Haga clic en **Siguiente** y, a continuación, en **Finalizar**.

Utilizar un host como plantilla para crear una configuración de redes uniforme en vSphere Distributed Switch

Si planifica incluir hosts con una configuración de redes uniforme, puede seleccionar un host como plantilla y aplicar su configuración para las NIC físicas y los adaptadores VMkernel a otros host del conmutador distribuido.

Procedimiento

1. En vSphere Web Client, desplácese hasta el conmutador distribuido.
2. En el menú **Acciones**, seleccione **Agregar y administrar hosts**.
3. Seleccione una tarea para la administración de redes de host y haga clic en **Siguiente**.
4. Seleccione los hosts que desea agregar o administrar en el conmutador distribuido.

5 En la parte inferior del cuadro de diálogo, seleccione **Configurar opciones de redes idénticas en varios hosts** y haga clic en **Siguiente**.

6 Seleccione un host para utilizarlo como plantilla y haga clic en **Siguiente**.

7 Seleccione las tareas del adaptador de red y haga clic en **Siguiente**.

8 En las páginas Administrar adaptadores de red físicos y Administrar adaptadores de red VMkernel, haga los cambios de configuración que necesite en el host de plantilla y, a continuación, haga clic en **Aplicar a todo** para todos los demás hosts.

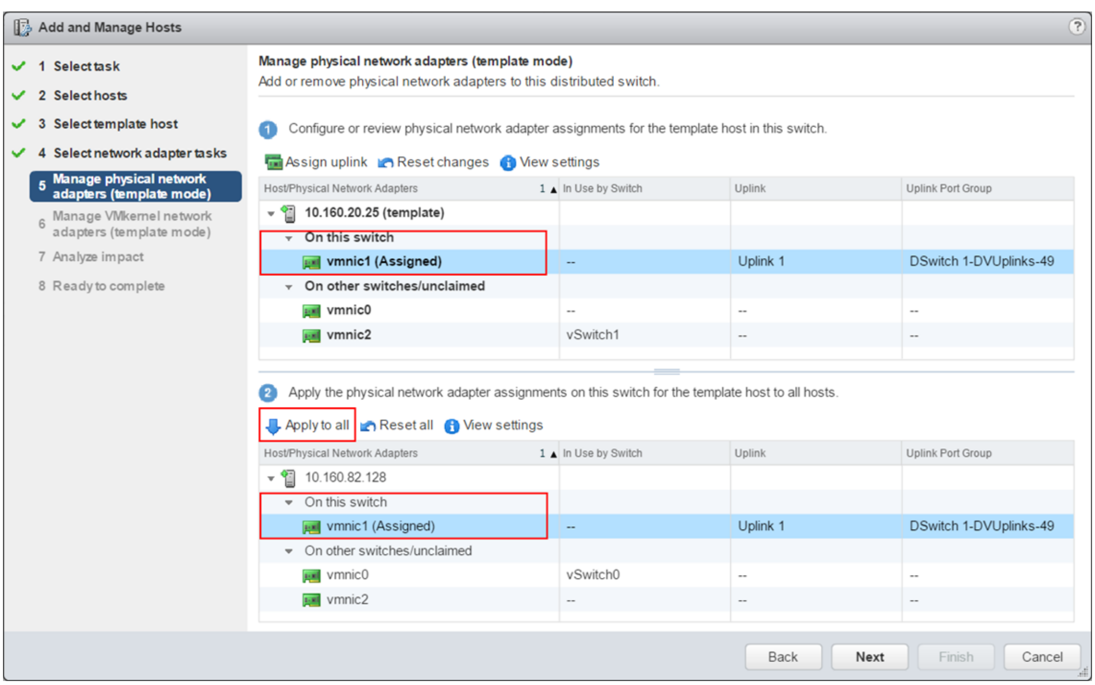
9 En la página Listo para finalizar, haga clic en **Finalizar**.

Ejemplo: Configurar adaptadores físicos y de VMkernel mediante un host de plantilla

Use el modo de host de plantilla del asistente para **agregar y administrar hosts** con el objetivo de crear una configuración de red uniforme en todos los hosts de un conmutador distribuido.

En la página Administrar adaptadores de red físicos del asistente, asigne una NIC física a un vínculo superior en el host de plantilla y, a continuación, haga clic en **Aplicar a todo** para crear la misma configuración en el otro host.

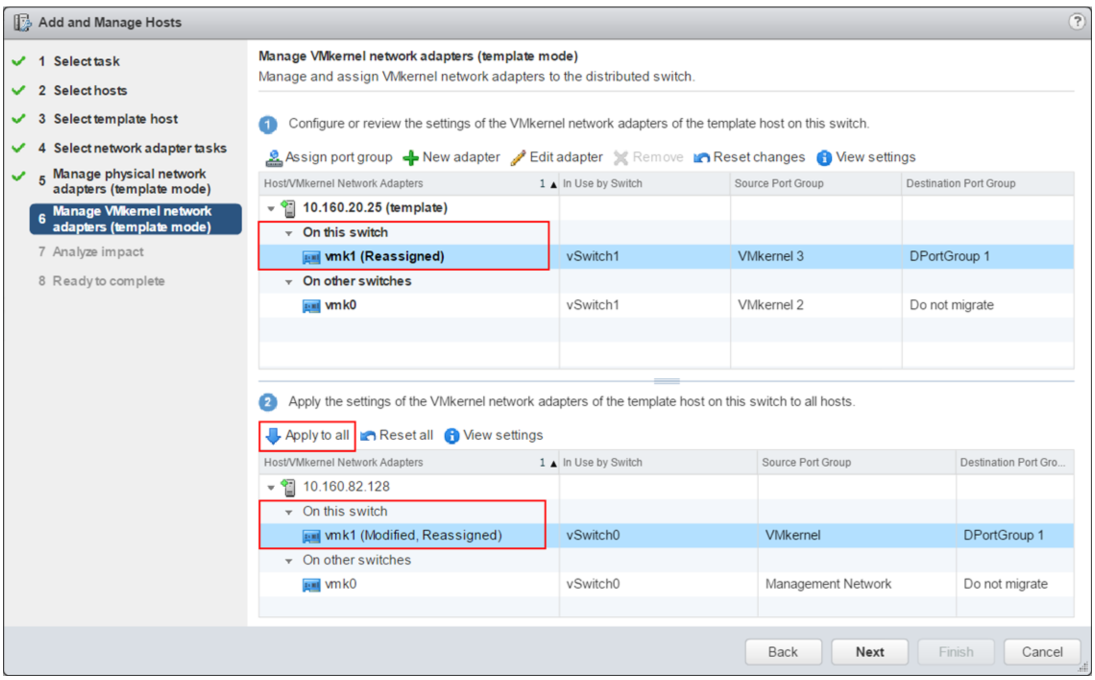
Figura 3-4. Aplicar la configuración de NIC físicas en vSphere Distributed Switch con un host de plantilla



En la página de administración de adaptadores de red de VMkernel, asigne un adaptador de VMkernel a un grupo de puertos y haga clic en **Aplicar a todo** para aplicar la misma configuración al otro host.

Tras hacer clic en el botón **Aplicar a todo**, el adaptador de VMkernel de destino tendrá los calificadores Modificado y Reasignado. El calificador Modificado aparece debido a que, cuando se hace clic en el botón **Aplicar a todo**, vCenter Server copia las especificaciones de configuración del adaptador de VMkernel de plantilla en el adaptador de VMkernel de destino aunque las configuraciones de los adaptadores de plantilla y de destino sean idénticas. Por lo tanto, los adaptadores de destino siempre se modifican.

Figura 3-5. Aplicar la configuración del adaptador de VMkernel a vSphere Distributed Switch mediante un host de plantilla



Quitar hosts de vSphere Distributed Switch

Quite los hosts de un conmutador distribuido de vSphere si configuró un conmutador diferente para los hosts.

Requisitos previos

- Compruebe que las NIC físicas de los hosts de destino se migren a otro conmutador.
- Compruebe que los adaptadores VMkernel de los hosts se migren a otro conmutador.
- Compruebe que los adaptadores de red de máquinas virtuales se migren a otro conmutador.

Para obtener más información sobre la migración de adaptadores de red a conmutadores diferentes, consulte Tareas para administrar redes de host en vSphere Distributed Switch.

Procedimiento

1 En vSphere Web Client, desplácese hasta el conmutador distribuido.

2 En el menú **Acciones**, seleccione **Agregar y administrar hosts**.

3 Seleccione **Quitar hosts** y haga clic en **Siguiente**.

4 Seleccione los hosts que desee quitar y haga clic en **Siguiente**.

5 Haga clic en **Finalizar**.

Administrar redes en conmutadores proxy de host

Puede modificar la configuración del conmutador proxy de cada host asociado con un conmutador distribuido de vSphere. Puede administrar las NIC físicas, los adaptadores VMkernel y los adaptadores de red de máquina virtual.

Para obtener información sobre cómo configurar redes VMkernel en conmutadores proxy de host, consulte Crear un adaptador VMkernel en vSphere Distributed Switch.

Migrar adaptadores de red en un host a Habilitar el protocolo Link Layer Discovery Protocol en vSphere Distributed Switch

Para los hosts asociados con un conmutador distribuido, es posible migrar los adaptadores de red de un conmutador estándar al conmutador distribuido. Puede migrar NIC físicas, adaptadores VMkernel y adaptadores de red de máquina virtual al mismo tiempo.

Para migrar los adaptadores de red de máquina virtual o los adaptadores VMkernel, asegúrese de que los grupos de puertos distribuidos de destino tengan al menos un vínculo superior activo que esté conectado a una NIC física en este host. Una alternativa es migrar las NIC físicas, los adaptadores de red virtuales y los adaptadores VMkernel de una vez.

Para migrar NIC físicas, asegúrese de que los grupos de puertos de origen del conmutador estándar tengan al menos una NIC física para controlar el tráfico. Por ejemplo, si migra una NIC física asignada a un grupo de puertos para la conexión de redes de máquina virtual, asegúrese de que el grupo de puertos tenga conexión con al menos una NIC física. En caso contrario, las máquinas virtuales de la misma VLAN del conmutador estándar tendrán conectividad entre sí, pero no se conectarán a la red externa.

Procedimiento

1 En vSphere Web Client, desplácese hasta el host.

2 En la pestaña **Configurar**, expanda **Redes** y seleccione **Conmutadores virtuales**.

3 Seleccione el conmutador distribuido de destino y haga clic en **Migrar adaptadores de red físicos o virtuales a este conmutador distribuido**.

4 Seleccione las tareas de migración de los adaptadores de red y haga clic en **Siguiente**.

5 Configure las NIC físicas.

   a En la lista **En otros conmutadores/sin reclamar**, seleccione una NIC física y haga clic en **Asignar vínculo superior**.

   b Seleccione un vínculo superior y haga clic en **Aceptar**.

   c Haga clic en **Siguiente**.

6 Configure los adaptadores VMkernel.

   a Seleccione un adaptador y haga clic en **Asignar grupo de puertos**.

   b Seleccione un grupo de puertos distribuidos y haga clic en **Aceptar**.

      Conecte un adaptador VMkernel a un grupo de puertos distribuidos por vez.

   c Haga clic en **Siguiente**.

7 Revise los servicios afectados por la nueva configuración de redes.

   a Si se informa un efecto importante o grave para un servicio, haga clic en el servicio y revise los detalles del análisis.

      Por ejemplo, en algunos casos se informa un impacto importante para iSCSI si hay un error en la configuración de formación de equipos y conmutación por error del grupo de puertos distribuidos donde se migra el adaptador VMkernel iSCSI. Debe dejar un vínculo superior activo en el orden de formación de equipos y conmutación por error del grupo de puertos distribuidos, dejar la lista de espera vacía y configurar los demás vínculos superiores como vínculos sin uso.

   b Después de solucionar cualquier problema de impacto para los servicios afectados, haga clic en **Siguiente**.

8 Configure los adaptadores de red de máquina virtual.

   a Seleccione una máquina virtual o un adaptador de red de máquina virtual y haga clic en **Asignar grupo de puertos**.

      Si selecciona una máquina virtual, se migran todos los adaptadores de red de la máquina virtual. Si selecciona un adaptador de red, se migra solamente el adaptador de red.

   b Seleccione un grupo de puertos distribuidos de la lista y haga clic en **Aceptar**.

   c Haga clic en **Siguiente**.

9 En la página Listo para finalizar, revise la nueva configuración de redes y haga clic en **Finalizar**.

Migrar un adaptador VMkernel de un host a vSphere Standard Switch

Si un host está asociado con un conmutador distribuido, puede migrar los adaptadores VMkernel del conmutador distribuido a un conmutador estándar.

Para obtener más información sobre la creación de adaptadores VMkernel en un conmutador distribuido de vSphere, consulte Crear un adaptador VMkernel en vSphere Distributed Switch.

Requisitos previos

Compruebe que el conmutador estándar de destino contenga al menos una NIC física.

Procedimiento

1 En vSphere Web Client, desplácese hasta el host.

2 En la pestaña **Configurar**, expanda **Redes** y seleccione **Conmutadores virtuales**.

3 Seleccione el conmutador estándar de destino en la lista.

4 Haga clic en **Migrar un adaptador de red de VMkernel al conmutador seleccionado**.

5 En la página Seleccionar adaptador de red VMkernel, seleccione en la lista el adaptador de red virtual que se migrará al conmutador estándar.

6 En la página Configurar opciones, modifique los valores de los campos **Etiqueta de red** e **Identificador de VLAN** para el adaptador de red.

7 En la página Listo para finalizar, revise los detalles de la migración y haga clic en **Finalizar**.

Haga clic en **Atrás** para modificar la configuración.

Asignar una NIC física de host a vSphere Distributed Switch

Puede asignar NIC físicas de un host asociado con un conmutador distribuido a un puerto de vínculo superior en el conmutador proxy del host.

Procedimiento

1 En vSphere Web Client, desplácese hasta el host.

2 En la pestaña **Configurar**, expanda **Redes** y seleccione **Conmutadores virtuales**.

3 Seleccione un conmutador distribuido de la lista.

4 Haga clic en el icono **Administrar los adaptadores de redes físicas conectados al conmutador seleccionado**.

5 Seleccione un vínculo superior libre de la lista y haga clic en **Agregar adaptador**.

6 Seleccione una NIC física y haga clic en **Aceptar**.

Quitar una NIC física de vSphere Distributed Switch

Puede quitar una NIC física de host desde un vínculo superior en un conmutador distribuido de vSphere.

Procedimiento

1 En vSphere Web Client, desplácese hasta el host.

2 En la pestaña **Configurar**, expanda **Redes** y seleccione **Conmutadores virtuales**.

3 Seleccione el conmutador distribuido.

4 Haga clic en el icono **Administrar los adaptadores de redes físicas conectados al conmutador seleccionado**.

5 Seleccione un vínculo superior y haga clic en **Quitar adaptadores seleccionados**.

6 Haga clic en **Aceptar**.

Pasos siguientes

Al quitar NIC físicas de máquinas virtuales activas, es posible que en vSphere Web Client se sigan mostrando estas NIC. Consulte Quitar las NIC de máquinas virtuales activas.

Quitar las NIC de máquinas virtuales activas

Al quitar las NIC de máquinas virtuales activas, es posible que en vSphere Web Client aún se puedan ver las NIC eliminadas.

Quitar las NIC de una máquina virtual activa sin tener instalado un sistema operativo invitado

No se pueden quitar las NIC de una máquina virtual activa que no tenga un sistema operativo instalado.

vSphere Web Client podría informar que la NIC se quitó, pero se seguirá viendo que está asociada a la máquina virtual.

Quitar las NIC de una máquina virtual activa con un sistema operativo invitado instalado

Se puede quitar una NIC de una máquina virtual activa, pero es posible que vSphere Web Client no lo informe durante algún tiempo. Al hacer clic en **Editar configuración** en la máquina virtual, es posible que vea la NIC eliminada incluso después de que la tarea se haya completado. La NIC eliminada no aparece inmediatamente en el cuadro de diálogo Editar configuración que corresponde a la máquina virtual.

Si el sistema operativo invitado de la máquina virtual no admite la eliminación en caliente de las NIC, es posible que se siga viendo la NIC asociada a la máquina virtual.

Grupos de puertos distribuidos

Un grupo de puertos distribuidos especifica las opciones de configuración de puerto de cada puerto miembro en un conmutador distribuido de vSphere. Los grupos de puertos distribuidos definen cómo se hace una conexión a una red.

Agregar un grupo de puertos distribuidos

Agregue un grupo de puertos distribuidos a vSphere Distributed Switch para crear una red de conmutador distribuido para las máquinas virtuales y asociar adaptadores VMkernel.

Procedimiento

1 En vSphere Web Client, desplácese hasta el conmutador distribuido.

2 Haga clic con el botón derecho en el conmutador distribuido y seleccione **Grupo de puertos distribuidos > Nuevo grupo de puertos distribuidos**.

3 En la página Seleccionar nombre y ubicación, introduzca el nombre del nuevo grupo de puertos distribuidos o acepte el nombre generado y, a continuación, haga clic en **Siguiente**.

4 En la página Configurar parámetros, establezca las propiedades generales para el nuevo grupo de puertos distribuidos y haga clic en **Siguiente**.

Configuración	Descripción
Enlace de puertos	Elija cuándo se deben asignar los puertos a las máquinas virtuales conectadas a este grupo de puertos distribuidos. ■ **Enlace estático**: asigna un puerto a una máquina virtual cuando la máquina virtual se conecta al grupo de puertos distribuidos. ■ **Enlace dinámico**: asigna un puerto a una máquina virtual la primera vez que la máquina virtual se enciende después de conectarla al grupo de puertos distribuidos. El enlace dinámico quedó obsoleto a partir de ESXi 5.0. ■ **Efímero - Sin enlace**: sin enlace de puertos. Puede asignar una máquina virtual a un grupo de puertos distribuidos con enlace de puertos efímero también cuando se conecta al host.
Asignación de puertos	■ **Elástica:** la cantidad predeterminada de puertos es ocho. Cuando se asignan todos los puertos, se crea un nuevo conjunto de ocho puertos. Esta es la opción predeterminada. ■ **Fija:** la cantidad predeterminada de puertos se establece en ocho. No se crean puertos adicionales cuando todos los puertos están asignados.
Cantidad de puertos	Introduzca la cantidad de puertos del grupo de puertos distribuidos.
Grupo de recursos de red	Use el menú desplegable para asignar el nuevo grupo de puertos distribuidos a un grupo de recursos de red definido por el usuario. Si no creó un grupo de recursos de red, el menú está vacío.
VLAN	Use el menú desplegable **Tipo de VLAN** para seleccionar las opciones de VLAN: ■ **Ninguna**: no utilice la VLAN. ■ **VLAN**: en el cuadro de texto **Identificador de VLAN**, escriba un número entre 1 y 4.094. ■ **Enlace troncal de VLAN**: escriba un rango troncal de VLAN. ■ **VLAN privada**: Seleccione una entrada de VLAN privada. Si no creó ninguna VLAN privada, este menú estará vacío.
Avanzado	Para personalizar las configuraciones de directiva para el nuevo grupo de puertos distribuidos, seleccione esta casilla.

5 (opcional) En la página Seguridad, modifique las excepciones de seguridad y haga clic en **Siguiente**.

Configuración	Descripción
Modo promiscuo	■ **Rechazar**. Colocar un adaptador en modo promiscuo desde el sistema operativo invitado no hace que se reciban tramas para otras máquinas virtuales. ■ **Aceptar**. Si se coloca un adaptador en modo promiscuo desde el sistema operativo invitado, el conmutador permite que el adaptador invitado reciba todas las tramas que pasan por el conmutador conforme a la directiva de VLAN activa para el puerto al que está conectado el adaptador. Los firewalls, los detectores de puertos y los sistemas de detección de intrusiones, entre otros, deben ejecutarse en modo promiscuo.
Cambios de dirección MAC	■ **Rechazar**. Si establece esta opción en **Rechazar**, y el sistema operativo invitado cambia la dirección MAC del adaptador a un valor diferente de la dirección establecida en el archivo de configuración `.vmx`, el conmutador descarta todas las tramas entrantes al adaptador de máquina virtual. Si el sistema operativo invitado vuelve a aplicar la dirección MAC anterior, la máquina virtual vuelve a recibir tramas. ■ **Aceptar**. Si el sistema operativo invitado cambia la dirección MAC de un adaptador de red, el adaptador recibe las tramas en su nueva dirección.
Transmisiones falsificadas	■ **Rechazar**. El conmutador descarta todas las tramas salientes que tengan una dirección MAC de origen diferente de la establecida en el archivo de configuración `.vmx`. ■ **Aceptar**. El conmutador no realiza el filtrado y permite todas las tramas salientes.

6 (opcional) En la sección Catalogación de tráfico, habilite o deshabilite Catalogación de tráfico de ingreso o Catalogación de tráfico de egreso y, a continuación, haga clic en **Siguiente**.

Configuración	Descripción
Estado	Si habilita **Catalogación de tráfico de ingreso** o **Catalogación de tráfico de egreso**, se establecen límites para la cantidad de ancho de banda de las redes asignada para cada adaptador virtual asociado a este grupo de puertos en particular. Si se deshabilita esta directiva, los servicios establecen una conexión libre y clara con la red física de forma predeterminada.
Ancho de banda promedio	Establece la cantidad de bits por segundo permitida para atravesar un puerto, promediada en el tiempo. Esta es la carga promedio permitida.

Configuración	Descripción
Ancho de banda máximo	La cantidad máxima de bits por segundo que se permitirá en un puerto para el envío o la recepción de una ráfaga de tráfico. Esta cantidad máxima supera el ancho de banda utilizado por un puerto cada vez que este utilice las ráfagas adicionales.
Tamaño de ráfaga	Es la cantidad máxima de bytes que se permiten en una ráfaga. Si se establece este parámetro, un puerto podría recibir una ráfaga adicional cuando no utiliza todo el ancho de banda asignado. Cada vez que el puerto necesite más ancho de banda que el especificado en **Ancho de banda promedio**, podrá transmitir temporalmente datos a una velocidad mayor si estuviera disponible una ráfaga adicional. Este parámetro establece la cantidad máxima de bytes que se pueden acumular en la ráfaga adicional y que se pueden transferir a una velocidad mayor.

7 (opcional) En la página Formación de equipos y conmutación por error, modifique la configuración y haga clic en **Siguiente**.

Configuración	Descripción
Equilibrio de carga	Especifique de qué forma elegir un vínculo superior. ■ **Enrutar según el puerto virtual de origen**. Elija un vínculo superior basado en el puerto virtual por donde el tráfico entró al conmutador distribuido. ■ **Enrutar según el hash de IP**. Elija un vínculo superior basado en un hash de las direcciones IP de origen y de destino de cada paquete. Para los paquetes que no utilizan IP, lo que se encuentre en estos desplazamientos se utiliza para calcular el hash. ■ **Enrutar según el hash de MAC de origen**. Elija un vínculo superior basado en un hash de la Ethernet de origen. ■ **Enrutar según la carga de la NIC física**. Elija un vínculo superior basado en las cargas actuales de las NIC físicas. ■ **Utilizar orden explícito de conmutación por error**. Utilice siempre el vínculo superior de orden más elevado de la lista de adaptadores activos, que cumpla los criterios de detección de conmutación por error. **Nota** La formación de equipos basada en IP requiere que el conmutador físico se configure con EtherChannel. Para las demás opciones, deshabilite EtherChannel.
Detección de errores de red	Especifique el método que se utilizará para la detección de conmutación por error. ■ **Solo estado de vínculo**: se basa solamente en el estado del vínculo que proporciona el adaptador de red. Esta opción detecta errores, como cables extraídos y errores de alimentación de conmutadores físicos, pero no errores de configuración, como puertos de conmutadores físicos bloqueados por árboles de expansión o configurados hacia la VLAN incorrecta, o cables extraídos en el otro extremo de un conmutador físico. ■ **Sondeo de señal**. Envía y escucha sondas de señal en todas las NIC del equipo, y utiliza esta información, además del estado del vínculo, para determinar el error en el vínculo. Se detectan muchos de los errores mencionados anteriormente que no pueden detectarse solo con el estado del vínculo. **Nota** No utilice sondeo de señal con equilibrio de carga de hash de IP.
Notificar a conmutadores	Seleccione **Sí** o **No** para notificar a los conmutadores en caso de una conmutación por error. Si selecciona **Sí**, siempre que haya una NIC virtual conectada al conmutador distribuido o siempre que el tráfico de la NIC virtual se enrute por otra NIC física en el equipo debido a un evento de conmutación por error, se envía una notificación a la red para actualizar las tablas de búsqueda en los conmutadores físicos. En casi todos los casos, este proceso se recomienda para la latencia más baja de casos de conmutación por error y migración con vMotion. **Nota** No utilice esta opción cuando las máquinas virtuales que utilizan el grupo de puertos estén utilizando el equilibrio de carga de red de Microsoft en modo de unidifusión. Este problema no existe cuando se ejecuta NLB en modo de multidifusión.

Configuración	Descripción
Conmutación por recuperación	Seleccione **Sí** o **No** para habilitar o deshabilitar la conmutación por recuperación. Esta opción determina de qué forma un adaptador físico vuelve a activarse después de recuperarse de un error. Si la conmutación por recuperación se establece en **Yes** (Sí) —predeterminado—, el adaptador vuelve a servicio activo inmediatamente después de recuperarse, desplazando a cualquier adaptador en espera que hubiera ocupado su ranura. Si la conmutación por recuperación se establece en **No**, un adaptador con errores se deja inactivo incluso después de la recuperación hasta que otro adaptador actualmente activo presente errores y requiera su sustitución.
Orden de conmutación por error	Especifique de qué forma se distribuye la carga de trabajo en los vínculos superiores. Para utilizar algunos vínculos superiores, pero reservar otros para emergencias en caso de que los vínculos superiores en uso presenten errores, establezca esta condición moviéndolos a diferentes grupos: ■ **Vínculos superiores activos**. Siga utilizando el vínculo superior si la conectividad del adaptador de red está activa y en funcionamiento. ■ **Vínculos superiores en espera**: utilice este vínculo superior si la conectividad de uno de los adaptadores activos está desactivada. ■ **Vínculos superiores sin utilizar**. No utilice este vínculo superior. **Nota** Cuando se utilice el equilibrio de carga de hash de IP, no configure vínculos superiores en espera.

8 (opcional) En la página Supervisión, habilite o deshabilite NetFlow y haga clic en **Siguiente**.

Configuración	Descripción
Deshabilitado	NetFlow está deshabilitado en el grupo de puertos distribuidos.
Habilitado	NetFlow está habilitado en el grupo de puertos distribuidos. Las opciones de NetFlow pueden configurarse en el nivel de vSphere Distributed Switch.

9 (opcional) En la página Varios, seleccione **Sí** o **No** y, a continuación, haga clic en **Siguiente**.

Si selecciona **Sí** se cierran todos los puertos en el grupo de puertos. Esta acción podría interrumpir las operaciones de red normales de los hosts o de las máquinas virtuales que utilicen los puertos.

10 (opcional) En la página Editar configuración adicional, agregue una descripción del grupo de puertos y establezca las anulaciones de directivas por puerto correspondientes; a continuación, haga clic en **Siguiente**.

11 En la página Listo para finalizar, revise su configuración y haga clic en **Finalizar**.

Para cambiar cualquier configuración, haga clic en el botón **Atrás** .

Editar la configuración general del grupo de puertos distribuidos

Se puede editar la configuración general del grupo de puertos distribuidos, como el nombre del grupo, la configuración de los puertos y el grupo de recursos de red.

Procedimiento

1 Busque un grupo de puertos distribuidos en vSphere Web Client.

   a Seleccione un conmutador distribuido y haga clic en la pestaña **Redes**.

   b Haga clic en **Grupos de puertos distribuidos**.

2 Haga clic con el botón derecho en el grupo de puertos distribuidos y seleccione **Editar configuración**.

3 Seleccione **General** para editar la configuración del grupo de puertos distribuidos siguiente.

Opción	Descripción
Nombre	Es el nombre del grupo de puertos distribuidos. Se puede editar el nombre en el campo de texto.
Enlace de puertos	Elija cuándo los puertos se deben asignar a las máquinas virtuales conectadas a este grupo de puertos distribuidos. ■ **Enlace estático**: asigna un puerto a una máquina virtual cuando la máquina virtual se conecta al grupo de puertos distribuidos. ■ **Enlace dinámico**: asigna un puerto a una máquina virtual la primera vez que la máquina virtual se enciende después de conectarla al grupo de puertos distribuidos. El enlace dinámico quedó obsoleto a partir de ESXi 5.0. ■ **Efímero**: sin enlace de puertos. También se puede asignar una máquina virtual a un grupo de puertos distribuidos con enlace de puertos efímeros mientras se está conectado al host.
Asignación de puertos	■ **Elástica:** la cantidad predeterminada de puertos se establece en ocho. Cuando se asignan todos los puertos, se crea un nuevo conjunto de ocho puertos. Esta es la opción predeterminada. ■ **Fija:** la cantidad predeterminada de puertos se establece en ocho. No se crean puertos adicionales cuando todos los puertos están asignados.
Cantidad de puertos	Introduzca la cantidad de puertos del grupo de puertos distribuidos.
Grupo de recursos de red	Use el menú desplegable para asignar el nuevo grupo de puertos distribuidos a un grupo de recursos de red definido por el usuario. Si no creó un grupo de recursos de red, el menú está vacío.
Descripción	Introduzca cualquier información sobre el grupo de puertos distribuidos en el campo de descripción.

4 Haga clic en **Aceptar**.

Quitar un grupo de puertos distribuidos

Quite un grupo de puertos distribuidos cuando ya no necesite que la red etiquetada correspondiente proporcione conectividad y configure las opciones de conexión para las máquinas virtuales o las redes VMkernel.

Requisitos previos

- Compruebe que todas las máquinas virtuales conectadas a la red etiquetada correspondiente se migren a una red etiquetada diferente.

- Compruebe que todos los adaptadores VMkernel conectados al grupo de puertos distribuidos se migren a un grupo de puertos diferente o se eliminen.

Procedimiento

1 Busque un grupo de puertos distribuidos en vSphere Web Client.

   a Seleccione un conmutador distribuido y haga clic en la pestaña **Redes**.

   b Haga clic en **Grupos de puertos distribuidos**.

2 Seleccione el grupo de puertos distribuidos.

3 En el menú **Acciones**, seleccione **Eliminar**.

Trabajar con puertos distribuidos

Un puerto distribuido es un puerto de un conmutador distribuido de vSphere que se conecta al VMkernel o al adaptador de red de una máquina virtual.

La configuración predeterminada del puerto distribuido queda determinada por las opciones del grupo de puertos distribuidos, aunque también es posible anular algunas opciones para los puertos distribuidos individuales.

Supervisar estado de los puertos distribuidos

vSphere puede supervisar los puertos distribuidos y proporcionar información sobre el estado actual y las estadísticas de tiempo de ejecución de cada puerto.

Procedimiento

1 Busque un grupo de puertos distribuidos en vSphere Web Client.

   a Seleccione un conmutador distribuido y haga clic en la pestaña **Redes**.

   b Haga clic en **Grupos de puertos distribuidos**.

2 Haga doble clic en un grupo de puertos distribuidos.

3 Haga clic en la pestaña **Puertos** y seleccione un puerto de la lista.

4 Haga clic en el icono **Iniciar supervisión de estado del puerto**.

   La tabla de puertos correspondiente al grupo de puertos distribuidos muestra las estadísticas de tiempo de ejecución de cada puerto distribuido.

   La columna **Estado** muestra el estado actual de cada puerto distribuido.

Opción	Descripción
Vínculo conectado	El vínculo de este puerto distribuido está conectado.
Vínculo desconectado	El vínculo de este puerto distribuido está desconectado.

Opción	Descripción
Bloqueado	Este puerto distribuido está bloqueado.
--	El estado de este puerto distribuido no está disponible en este momento.

Configurar opciones de puertos distribuidos

Se puede cambiar la configuración general de puertos distribuidos, como el nombre y la descripción del puerto.

Procedimiento

1 Busque un grupo de puertos distribuidos en vSphere Web Client.

  a Seleccione un conmutador distribuido y haga clic en la pestaña **Redes**.

  b Haga clic en **Grupos de puertos distribuidos**.

2 Haga doble clic en un grupo de puertos distribuidos en la lista.

3 Haga clic en la pestaña **Puertos** y seleccione un puerto distribuido de la tabla.

  En la sección inferior de la pantalla, se muestra información sobre el puerto distribuido.

4 Haga clic en el icono **Editar configuración de puertos distribuidos**.

5 En la página Propiedades y en las páginas de directivas, edite la información sobre el puerto distribuido y haga clic en **Aceptar**.

  Si no se permite la anulación, se deshabilitan las opciones de la directiva.

  Para permitir las anulaciones en el nivel de los puertos, puede cambiar las opciones de la sección **Configuración avanzada** del grupo de puertos distribuidos. Consulte Configurar las directivas de red de anulación en los puertos.

Configurar redes de una máquina virtual en vSphere Distributed Switch

Conecte las máquinas virtuales a un conmutador distribuido de vSphere ya sea mediante la configuración de la NIC de una máquina virtual individual o la migración de grupos de máquinas virtuales desde el propio conmutador distribuido de vSphere.

Para conectar las máquinas virtuales a conmutadores distribuidos de vSphere, conecte los adaptadores de red virtuales asociados a los grupos de puertos distribuidos. Para una máquina virtual individual, puede hacerlo modificando la configuración del adaptador de red de la máquina, o bien para un grupo de máquinas virtuales, migrando las máquinas desde una red virtual existente a un conmutador distribuido de vSphere.

Migrar máquinas virtuales desde o hacia vSphere Distributed Switch

Además de conectar las máquinas virtuales a un conmutador distribuido a nivel de máquina virtual individual, puede migrar un grupo de máquinas virtuales entre una red de vSphere Distributed Switch y una red de vSphere Standard Switch.

Procedimiento

1 En vSphere Web Client, desplácese hasta un centro de datos.

2 Haga clic con el botón derecho en el centro de datos del navegador y seleccione **Migrar máquina virtual a otra red**.

3 Seleccione una red de origen.

   - Seleccione **Red específica** y use el botón **Examinar** para seleccionar una red de origen específica.
   - Seleccione **Sin red** para migrar todos los adaptadores de red de máquina virtual que no estén conectados a ninguna otra red.

4 Use **Examinar** para seleccionar una red de destino y haga clic en **Siguiente**.

5 Seleccione las máquinas virtuales de la lista para migrar desde la red de origen hacia la red de destino y, a continuación, haga clic en **Siguiente**.

6 Revise las selecciones y haga clic en **Finalizar**.

   Haga clic en **Atrás** para modificar las selecciones.

Conectar una máquina virtual individual a un grupo de puertos distribuidos

Para conectar una máquina virtual individual a vSphere Distributed Switch, modifique la configuración de la NIC de la máquina virtual.

Procedimiento

1 Ubique la máquina virtual en vSphere Web Client.

   a Seleccione un centro de datos, una carpeta, un clúster, un grupo de recursos o un host y haga clic en la pestaña **Máquinas virtuales**.

   b Haga clic en **Máquinas virtuales** y haga doble clic en la máquina virtual en la lista.

2 En la pestaña **Configurar** de la máquina virtual, expanda **Configuración** y seleccione **Hardware de máquina virtual**.

3 Haga clic en **Editar**.

4 Expanda la sección **Adaptador de red** y seleccione **Mostrar más redes** en el menú desplegable **Adaptador de red**.

5 En el cuadro de diálogo Seleccionar red, seleccione un grupo de puertos distribuidos y haga clic en **Aceptar**.

6 Haga clic en **Aceptar**.

Diagramas de topología de vSphere Distributed Switch en vSphere Web Client

Los diagramas de topología de vSphere Distributed Switch en vSphere Web Client muestran la estructura de los adaptadores de máquinas virtuales, adaptadores VMkernel y adaptadores físicos del conmutador.

Se pueden examinar los componentes, dispuestos en grupos de puertos, cuyo tráfico es controlado por el conmutador, así como las conexiones entre ellos. El diagrama muestra información sobre el adaptador físico que conecta los adaptadores virtuales con la red externa.

Es posible ver los componentes que están en ejecución en todo el conmutador distribuido y en cada host que lo integra.

Observe el vídeo sobre las operaciones que se pueden realizar a partir del diagrama de topología de vSphere Distributed Switch.

Manejar redes virtuales mediante el diagrama de topología de VDS (https://vmwaretv.vmware.com/media/t/1_9umngsr4)

Diagrama de topología central

Se puede utilizar el diagrama de topología central del conmutador para ubicar y editar la configuración de los grupos de puertos distribuidos y los grupos de vínculos superiores asociados con varios hosts. Se puede iniciar la migración de los adaptadores de máquinas virtuales desde un grupo de puertos hasta un destino en el mismo conmutador o en otro distinto. También es posible reorganizar los hosts y sus redes en el conmutador mediante el asistente **Agregar y administrar hosts**.

Diagrama de topología del conmutador proxy de un host

El diagrama de topología del conmutador proxy de un host muestra los adaptadores conectados a los puertos de conmutador del host. Se puede editar la configuración de los adaptadores físicos y VMkernel.

Filtros del diagrama

Se pueden utilizar los filtros del diagrama para limitar la información que aparece en los diagramas de topología. El filtro predeterminado limita el diagrama de topología para que muestre 32 grupos de puertos, 32 hosts y 1.024 máquinas virtuales.

Para cambiar el ámbito del diagrama, es posible no utilizar filtros o aplicar filtros personalizados. Al utilizar un filtro personalizado, se puede ver la información únicamente de un conjunto de máquinas virtuales, de un conjunto de grupos de puertos en ciertos hosts, o de un puerto. Es posible crear filtros a partir del diagrama de topología central del conmutador distribuido.

Ver la topología de vSphere Distributed Switch

Examine la organización de los componentes que están conectados al conmutador distribuido a través de los hosts en vCenter Server.

Procedimiento

1 Desplácese hasta el conmutador distribuido de vSphere en vSphere Web Client.

2 En la pestaña **Configurar**, expanda **Configuraciones** y seleccione**Topología**.

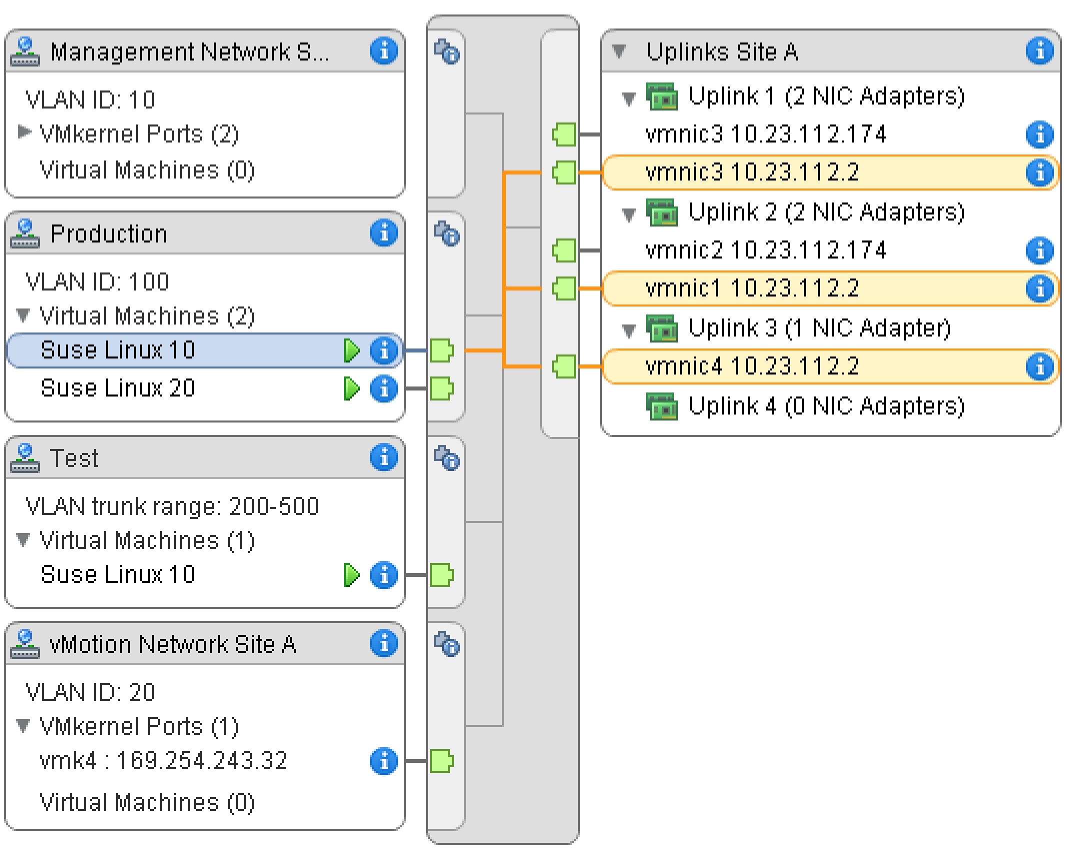
Resultados

De forma predeterminada, el diagrama muestra un máximo de 32 grupos de puertos distribuidos, 32 hosts y 1024 máquinas virtuales.

Ejemplo: Diagrama de un conmutador distribuido que conecta el VMkernel y las máquinas virtuales a la red

En su entorno virtual, vSphere Distributed Switch controla adaptadores VMkernel para vSphere vMotion y para la red de administración y las máquinas virtuales agrupadas. Es posible utilizar el diagrama de topología central para examinar si una máquina virtual o un adaptador VMkernel están conectados a la red externa y para identificar el adaptador físico que transporta los datos.

Figura 3-6. Diagrama de topología de un conmutador distribuido que controla el VMkernel y las redes de máquinas virtuales



Pasos siguientes

Es posible realizar las siguientes tareas comunes en la topología del conmutador distribuido:

- Utilice filtros para ver los componentes de redes solo para grupos de puertos seleccionados en determinados hosts, para máquinas virtuales seleccionadas o para un puerto.
- Ubique, configure y migre componentes de redes de las máquinas virtuales en grupos de puertos y hosts mediante el asistente **Migrar redes de máquinas virtuales**.
- Detecte los adaptadores de las máquinas virtuales que no tienen ninguna red asignada, y muévalos al grupo de puertos seleccionado mediante el asistente **Migrar redes de máquinas virtuales**.
- Controle los componentes de redes en varios hosts mediante el asistente **Agregar y administrar hosts**.
- Vea el equipo NIC o la NIC física que lleva el tráfico relacionado con un adaptador de máquina virtual seleccionada o con un adaptador VMkernel.

  De esta manera, también podrá ver el host en el que reside un adaptador VMkernel seleccionado. Seleccione el adaptador, rastree la ruta a la NIC física asociada y vea la dirección IP o el nombre de dominio junto a la NIC.
- Determine el modo y el identificador de VLAN correspondiente a un grupo de puertos. Para obtener información sobre los modos de VLAN, consulte Configuración de VLAN.

Ver la topología de un conmutador proxy del host

Examine y reorganice las redes del VMkernel y las máquinas virtuales que vSphere Distributed Switch controla en un host.

Procedimiento

1. En vSphere Web Client, desplácese hasta el host.
2. En la pestaña **Configurar**, expanda **Redes** y seleccione **Conmutadores virtuales**.
3. Seleccione un conmutador distribuido de la lista.

Resultados

La topología del conmutador proxy del host aparece en la lista.

Configurar redes VMkernel

4

Puede configurar los adaptadores VMkernel para que proporcionen conectividad de red a los hosts y procesen el tráfico del sistema de vMotion, almacenamiento IP, registros de Fault Tolerance, vSAN, entre otros.

- Capa de redes VMkernel

  La capa de redes VMkernel ofrece conectividad a los hosts y maneja el tráfico de sistema estándar de vSphere vMotion, el almacenamiento IP, Fault Tolerance, vSAN y otros. También puede crear adaptadores VMkernel en los hosts de vSphere Replication de origen y destino para aislar el tráfico de datos de replicación.

- Ver información sobre los adaptadores VMkernel en un host

  Puede ver los servicios asignados, el conmutador asociado, la configuración de puertos, las opciones de IP, la pila de TCP/IP, el identificador de VLAN y las directivas de cada adaptador VMkernel.

- Crear un adaptador VMkernel en vSphere Standard Switch

  Cree un adaptador de red VMkernel en un conmutador de vSphere Standard para proporcionar conectividad de red a los hosts y manejar el tráfico del sistema correspondiente a vSphere vMotion, almacenamiento IP, registro de Fault Tolerance, vSAN, entre otros. También puede crear adaptadores VMkernel en los hosts de vSphere Replication de origen y destino para aislar el tráfico de datos de replicación. Asigne un adaptador VMkernel a un solo tipo de tráfico.

- Crear un adaptador VMkernel en un host asociado con vSphere Distributed Switch

  Puede crear un adaptador VMkernel en un host asociado con un conmutador distribuido para brindar conectividad de red al host y controlar el tráfico de vSphere vMotion, almacenamiento IP, registro de Fault Tolerance, vSAN, y otros. Puede configurar adaptadores VMkernel para el tráfico del sistema estándar en los conmutadores estándar de vSphere y en los conmutadores distribuidos de vSphere.

- Editar la configuración del adaptador VMkernel

  Puede ser necesario modificar el tipo de tráfico admitido para un adaptador VMkernel o la forma en que se obtienen las direcciones IPv4 o IPv6.

- Anular la puerta de enlace predeterminada de un adaptador de VMkernel

  Es posible que necesite anular la puerta de enlace predeterminada de un adaptador de VMkernel para proporcionar otra puerta de enlace para vSphere vMotion.

- Configurar la puerta de enlace de un adaptador de VMkernel mediante comandos ESXCLI

  Puede anular la puerta de enlace predeterminada de un adaptador de VMkernel para proporcionar otra puerta de enlace de vSphere vMotion mediante los comandos ESXCLI.

- Ver la configuración de la pila de TCP/IP en un host

  Puede ver la configuración de DNS y de enrutamiento de una pila de TCP/IP en un host. También puede ver las tablas de enrutamiento IPv4 y IPv6, el algoritmo de control de congestión y la cantidad máxima de conexiones permitidas.

- Cambiar la configuración de una pila de TCP/IP en un host

  Puede cambiar la configuración de DNS y de la puerta de enlace predeterminada de una pila de TCP/IP en un host. También puede cambiar el algoritmo de control de congestión, la cantidad máxima de conexiones y el nombre de las pilas de TCP/IP personalizadas.

- Crear una pila de TCP/IP personalizada

  Puede crear una pila de TCP/IP personalizada en un host para reenviar el tráfico de redes a través de una aplicación personalizada.

- Quitar un adaptador VMkernel

  Quite un adaptador VMkernel de un conmutador distribuido o estándar de vSphere cuando ya no lo necesite. Asegúrese de dejar al menos un adaptador VMkernel para el tráfico de administración en el host a fin de mantener la conectividad de red.

Capa de redes VMkernel

La capa de redes VMkernel ofrece conectividad a los hosts y maneja el tráfico de sistema estándar de vSphere vMotion, el almacenamiento IP, Fault Tolerance, vSAN y otros. También puede crear adaptadores VMkernel en los hosts de vSphere Replication de origen y destino para aislar el tráfico de datos de replicación.

Pilas de TCP/IP en el nivel de VMkernel

Pila de TCP/IP predeterminada

Ofrece compatibilidad con redes para el tráfico de administración entre vCenter Server y los hosts ESXi, y para el tráfico de sistema en vMotion, el almacenamiento IP, Fault Tolerance, etc.

Pila de TCP/IP de vMotion

Admite el tráfico para la migración en vivo de máquinas virtuales. Use la pila de TCP/IP de vMotion para optimizar el aislamiento de tráfico de vMotion. Después de crear un adaptador de VMkernel en la pila de TCP/IP de vMotion, solamente puede usar esta pila para vMotion en este host. Los adaptadores de VMkernel en la pila de TCP/IP predeterminada se deshabilitan para el servicio de vMotion. Si una migración en vivo utiliza la pila de TCP/IP

predeterminada mientras se configuran los adaptadores VMkernel con la pila de TCP/IP de vMotion, la migración se completa correctamente. Sin embargo, los adaptadores de VMkernel involucrados en la pila de TCP/IP predeterminada se deshabilitan para las sesiones futuras de vMotion.

Pila de TCP/IP de aprovisionamiento

Admite el tráfico para una operación de migración de instantáneas, clonación o migración en frío de una máquina virtual. Puede usar la pila de TCP/IP de aprovisionamiento para manejar el tráfico de copias de archivos de red (NFC) durante operaciones de vMotion a larga distancia. NFC proporciona un servicio de FTP específico del tipo de archivo para vSphere. ESXi usa NFC para la copia y la transferencia de datos entre almacenes de datos. Los adaptadores VMkernel configurados con la pila de TCP/IP de aprovisionamiento manejan el tráfico de las operaciones de clonación de discos virtuales de las máquinas virtuales migradas en vMotion a larga distancia. Al usar la pila de TCP/IP de aprovisionamiento, es posible aislar el tráfico de las operaciones de clonación en una puerta de enlace independiente. Después de configurar un adaptador VMkernel con la pila de TCP/IP de aprovisionamiento, todos los adaptadores de la pila de TCP/IP predeterminada se deshabilitan para el tráfico de aprovisionamiento.

Pilas de TCP/IP personalizadas

Es posible agregar pilas de TCP/IP personalizadas en el nivel de VMkernel para manejar el tráfico de red de las aplicaciones personalizadas.

Proteger el tráfico de sistema

Tome las medidas de seguridad correspondientes para impedir el acceso no autorizado al tráfico de administración y del sistema en el entorno de vSphere. Por ejemplo, aísle el tráfico de vMotion en una red independiente que incluya únicamente los hosts ESXi que participan en la migración. Aísle el tráfico de administración en una red a la cual solo tengan acceso los administradores de red y de seguridad. Para obtener más información, consulte *Seguridad de vSphere* e *Instalar y configurar vSphere*.

Tipos de tráfico de sistema

Deberá asignar un adaptador de VMkernel exclusivo para cada tipo de tráfico. En el caso de los conmutadores distribuidos, asigne un grupo de puertos distribuidos específico a cada adaptador VMkernel.

Tráfico de administración

Transmite la comunicación de configuración y administración de los hosts ESXi, vCenter Server y el tráfico de host a host de High Availability. De forma predeterminada, al instalar el software ESXi, se crea vSphere Standard Switch en el host junto con un adaptador VMkernel para el

tráfico de administración. Para ofrecer redundancia, puede conectar dos o más NIC físicas a un adaptador VMkernel para el tráfico de administración.

Tráfico de vMotion

Admite vMotion. Se necesita un adaptador VMkernel para vMotion en los hosts de origen y de destino. Configure los adaptadores de VMkernel para vMotion de modo que solamente manejen el tráfico de vMotion. Para lograr un mejor rendimiento, se puede configurar vMotion con varias NIC. Para usar vMotion con varias NIC, puede asignar dos o más grupos de puertos exclusivos al tráfico de vMotion; cada grupo de puertos debe tener un adaptador de VMkernel de vMotion asociado. A continuación, se pueden conectar una o varias NIC físicas a cada grupo de puertos. De esta forma, se usan varias NIC físicas para vMotion, con lo cual se obtiene un ancho de banda mayor.

Nota El tráfico de red de vMotion no se cifra. Debe aprovisionar redes privadas seguras que solo vMotion pueda utilizar.

Tráfico de aprovisionamiento

Controla los datos que se transfieren para una operación de migración de instantáneas, clonación o migración en frío de una máquina virtual.

Tráfico y detección de almacenamiento IP

Controla la conexión de los tipos de almacenamiento que usan redes TCP/IP estándar y dependen de las redes VMkernel. Algunos de estos tipos de almacenamiento son iSCSI de software, iSCSI de hardware dependiente y NFS. Si tiene dos o más NIC físicas para iSCSI, puede configurar iSCSI con múltiples rutas. Los hosts ESXi admiten NFS 3 y 4.1. Para configurar un adaptador de canal de fibra en Ethernet (FCoE) de software, es preciso contar con un adaptador de VMkernel exclusivo. El adaptador FCoE de software transmite la información de configuración a través del protocolo Data Center Bridging Exchange (DCBX) mediante el módulo de VMkernel del protocolo Cisco Discovery Protocol (CDP).

Tráfico de Fault Tolerance

Controla los datos que la máquina virtual principal con tolerancia a errores envía a la máquina virtual secundaria con tolerancia a errores a través de la capa de redes VMkernel. Se necesita un adaptador VMkernel independiente para el registro de Fault Tolerance en cada host que forme parte de un clúster de vSphere HA.

Tráfico de vSphere Replication

Controla los datos de replicación salientes que el host ESXi de origen transmite al servidor de vSphere Replication. Asigne un adaptador VMkernel exclusivo en el sitio de origen para aislar el tráfico de replicación saliente.

Tráfico NFC de vSphere Replication

Controla los datos de replicación entrantes en el sitio de replicación de destino.

Tráfico de vSAN

Cada host que forma parte de un clúster de vSAN debe tener un adaptador VMkernel para manejar el tráfico de vSAN.

Ver información sobre los adaptadores VMkernel en un host

Puede ver los servicios asignados, el conmutador asociado, la configuración de puertos, las opciones de IP, la pila de TCP/IP, el identificador de VLAN y las directivas de cada adaptador VMkernel.

Procedimiento

1 En vSphere Web Client, desplácese hasta el host.

2 Haga clic en la pestaña **Configurar** y expanda el menú **Redes**.

3 Para ver información sobre todos los adaptadores VMkernel del host, seleccione **Adaptadores VMkernel**.

4 Seleccione un adaptador de la lista de adaptadores VMkernel para ver su configuración.

Tabulador	Descripción
Todo	Muestra toda la información de configuración del adaptador VMkernel. Incluye las opciones de configuración de puertos y NIC, de IPv4 y IPv6 y las directivas de catalogación de tráfico, de formación de equipos y conmutación por error, y de seguridad.
Propiedades	Muestra las propiedades del puerto y la configuración de NIC del adaptador VMkernel. Las propiedades de puerto incluyen el grupo de puertos (etiqueta de red) al cual está asociado el adaptador, el identificador de VLAN y los servicios habilitados. La configuración de NIC incluye la dirección MAC y el tamaño de MTU establecido.
Configuración de IP	Muestra todas las opciones de configuración de IPv4 o IPv6 para el adaptador VMkernel. No se muestra información de IPv6 si no se habilitó IPv6 en el host.
Directivas	Muestra las directivas de catalogación de tráfico, formación de equipos y conmutación por error, y seguridad que se aplican al grupo de puertos al cual está conectado el adaptador VMkernel.

Crear un adaptador VMkernel en vSphere Standard Switch

Cree un adaptador de red VMkernel en un conmutador de vSphere Standard para proporcionar conectividad de red a los hosts y manejar el tráfico del sistema correspondiente a vSphere vMotion, almacenamiento IP, registro de Fault Tolerance, vSAN, entre otros. También puede crear adaptadores VMkernel en los hosts de vSphere Replication de origen y destino para aislar el tráfico de datos de replicación. Asigne un adaptador VMkernel a un solo tipo de tráfico.

Procedimiento

1 En vSphere Web Client, desplácese hasta el host.

2 En la pestaña**Configurar**, expanda **Redes** y seleccione **Adaptadores de VMKernel**.

3 Haga clic en **Agregar redes de host**.

4 En la página Seleccionar tipo de conexión, seleccione **Adaptadores de red de VMkernel** y haga clic en **Siguiente**.

5 En la página Seleccionar dispositivo de destino, seleccione un conmutador estándar existente o seleccione **Nuevo conmutador estándar**.

6 (opcional) En la página Crear un conmutador estándar, asigne NIC físicas al conmutador.

   Puede crear el conmutador estándar sin NIC físicas y configurarlas más tarde. Durante el momento en que no hay NIC físicas asociadas al host, el host no tiene conectividad de red con los otros hosts en la red física. Las máquinas virtuales en el host pueden comunicarse entre sí.

   a Haga clic en **Agregar adaptadores** y seleccione tantas NIC físicas como necesite.

   b Utilice las flechas arriba y abajo para configurar las NIC activas y en espera.

7 En la página Propiedades de puerto, establezca la configuración para el adaptador de VMkernel.

Opción	Descripción
Etiqueta de red	Escriba un valor en esta etiqueta para indicar el tipo de tráfico correspondiente al adaptador VMkernel, por ejemplo **`Management traffic`** o **`vMotion`**.
identificador de VLAN	Establezca un identificador de VLAN para identificar la VLAN que utilizará el tráfico de red del adaptador VMkernel.
configuración de IP	Seleccione IPv4, IPv6 o ambas. **Nota** La opción IPv6 no aparece en los hosts en los que no se ha habilitado IPv6.

Opción	Descripción
Pila de TCP/IP	Seleccione una pila de TCP/IP de la lista. Después de establecer una pila de TCP/IP para el adaptador VMkernel, no es posible cambiarla más adelante. Si selecciona vMotion o la pila de TCP/IP de aprovisionamiento, podrá utilizar solo esta pila para controlar vMotion o el tráfico de aprovisionamiento en el host. Todos los adaptadores de VMkernel para vMotion en la pila de TCP/IP predeterminada se deshabilitan para las sesiones futuras de vMotion. Si utiliza la pila de TCP/IP de aprovisionamiento, los adaptadores VMkernel en la pila de TCP/IP predeterminada quedarán desactivados para las operaciones que incluyen el tráfico de aprovisionamiento, tales como las operaciones de migración de instantáneas, clonación o migración en frío de una máquina virtual.
Habilitación de servicios	Es posible habilitar servicios para la pila de TCP/IP predeterminada en el host. Seleccione una opción entre los servicios disponibles: ■ **Tráfico de vMotion**. Permite al adaptador de VMkernel anunciarse a otro host como la conexión de red mediante la cual se envía el tráfico de vMotion. La migración con vMotion al host seleccionado no es posible si el servicio vMotion no está habilitado para cualquier adaptador VMkernel en la pila de TCP/IP predeterminada, o si no hay adaptadores que estén utilizando la pila de TCP/IP de vMotion. ■ **Tráfico de aprovisionamiento**. Controla los datos que se transfieren para una operación de migración de instantáneas, clonación o migración en frío de una máquina virtual. ■ **Tráfico de Fault Tolerance**. Permite registrar Fault Tolerance en el host. Solamente se puede usar un adaptador de VMkernel por host para el tráfico de FT. ■ **Tráfico de administración**. Habilita el tráfico de administración del host y vCenter Server. Normalmente, se crea un adaptador VMkernel de este tipo para los hosts cuando se instala el software ESXi. Es posible crear otro adaptador de VMkernel para el tráfico de administración en el host con la finalidad de proporcionar redundancia. ■ **Tráfico de vSphere Replication**. Controla los datos de replicación salientes que se envían desde el host ESXi de origen al servidor de replicación de vSphere. ■ **Tráfico NFC de vSphere Replication**. Controla los datos de replicación entrantes en el sitio de replicación de destino. ■ **vSAN**. Habilita el tráfico de vSAN en el host. Todos los hosts que forman parte de un clúster de vSAN deben tener un adaptador de VMkernel de este tipo.

8 Si ha seleccionado las pilas TCP/IP de vMotion o Aprovisionamiento, haga clic en **Aceptar** en el cuadro de diálogo de advertencia que aparece.

Si ya se ha iniciado una operación de migración activa, esta se ejecuta correctamente incluso después de que se deshabilitan los adaptadores de VMkernel involucrados en la pila de TCP/IP predeterminada de vMotion. Lo mismo ocurre con las operaciones que incluyen adaptadores de VMkernel en la pila de TCP/IP predeterminada que están configurados para tráfico de aprovisionamiento.

9 (opcional) En la página Configuración de IPv4, seleccione una opción para obtener las direcciones IP.

Opción	Descripción
Obtener configuración de IPv4 automáticamente	Use DHCP para obtener la configuración de IP. Debe haber un servidor DHCP presente en la red.
Usar configuración de IPv4 estática	Escriba la dirección IP de IPv4 y la máscara de subred para el adaptador VMkernel. Las direcciones de servidor DNS y puerta de enlace predeterminada de VMkernel para IPv4 se obtienen de la pila TCP/IP seleccionada. Active la casilla **Anular la puerta de enlace predeterminada para este adaptador** e introduzca una dirección de puerta de enlace, en caso de que desee especificar una puerta de enlace diferente para el adaptador de VMkernel.

10 (opcional) En la página Configuración de IPv6, seleccione una opción para obtener las direcciones IPv6.

Opción	Descripción
Obtener las direcciones IPv6 automáticamente por medio de DHCP	Use DHCP para obtener las direcciones IPv6. Debe haber un servidor DHCPv6 presente en la red.
Obtener las direcciones IPv6 automáticamente por medio del anuncio de enrutador	Use el anuncio de enrutador para obtener las direcciones IPv6. En ESXi 6.5 y versiones posteriores, el anuncio de enrutador está habilitado de manera predeterminada, y se admiten las marcas M y O según RFC 4861.
Direcciones IPv6 estáticas	a Haga clic en **Agregar dirección IPv6** para agregar una nueva dirección IPv6. b Introduzca la dirección IPv6 y la longitud del prefijo de subred, y haga clic en **Aceptar**. c Para cambiar la puerta de enlace predeterminada de VMkernel, haga clic en **Anular la puerta de enlace predeterminada para este adaptador**. La dirección de puerta de enlace predeterminada de VMkernel para IPv6 se obtiene de la pila de TCP/IP seleccionada.

11 Revise las selecciones de configuración en la página Listo para finalizar y haga clic en **Finalizar**.

Crear un adaptador VMkernel en un host asociado con vSphere Distributed Switch

Puede crear un adaptador VMkernel en un host asociado con un conmutador distribuido para brindar conectividad de red al host y controlar el tráfico de vSphere vMotion, almacenamiento IP, registro de Fault Tolerance, vSAN, y otros. Puede configurar adaptadores VMkernel para el tráfico del sistema estándar en los conmutadores estándar de vSphere y en los conmutadores distribuidos de vSphere.

Debe asignar un grupo de puertos distribuidos exclusivo por adaptador VMkernel. Si desea lograr un mejor aislamiento, configure un adaptador VMkernel con un tipo de tráfico.

Procedimiento

1. En vSphere Web Client, desplácese hasta el host.
2. En la pestaña**Configurar**, expanda **Redes** y seleccione **Adaptadores de VMKernel**.
3. Haga clic en **Agregar redes de host**.
4. En la página Seleccionar tipo de conexión, seleccione **Adaptadores de red de VMkernel** y haga clic en **Siguiente**.
5. En la opción **Seleccionar una red existente**, seleccione un grupo de puertos distribuidos y haga clic en **Siguiente**.
6. En la página Propiedades de puerto, establezca la configuración para el adaptador de VMkernel.

Opción	Descripción
Etiqueta de red	La etiqueta de red se hereda de la etiqueta del grupo de puertos distribuidos.
configuración de IP	Seleccione IPv4, IPv6 o ambas. **Nota** La opción IPv6 no aparece en los hosts en los que no se ha habilitado IPv6.

Opción	Descripción
Pila de TCP/IP	Seleccione una pila de TCP/IP de la lista. Una vez que se configura una pila de TCP/IP para el adaptador de VMkernel, no es posible cambiarla posteriormente. Si selecciona la pila de TCP/IP de aprovisionamiento o de vMotion, solamente podrá usar estas pilas para controlar el tráfico de vMotion o de aprovisionamiento en el host. Todos los adaptadores de VMkernel para vMotion en la pila de TCP/IP predeterminada se deshabilitan para las sesiones futuras de vMotion. Si configura la pila de TCP/IP de aprovisionamiento, los adaptadores de VMkernel en la pila de TCP/IP predeterminada se deshabilitan para las operaciones que incluyan tráfico de aprovisionamiento, como una operación de migración de instantáneas, clonación o migración en frío de una máquina virtual.
Habilitación de servicios	Es posible habilitar servicios para la pila de TCP/IP predeterminada en el host. Seleccione una opción entre los servicios disponibles: ■ **Tráfico de vMotion**. Permite al adaptador de VMkernel anunciarse a otro host como la conexión de red mediante la cual se envía el tráfico de vMotion. La migración con vMotion al host seleccionado no es posible si el servicio de vMotion no se ha habilitado para ningún adaptador de VMkernel en la pila de TCP/IP predeterminada, ni tampoco si no hay adaptadores que estén utilizando la pila de TCP/IP de vMotion. ■ **Tráfico de aprovisionamiento**. Controla los datos que se transfieren para una operación de migración de instantáneas, clonación o migración en frío de una máquina virtual. ■ **Tráfico de Fault Tolerance**. Permite registrar Fault Tolerance en el host. Solamente se puede usar un adaptador de VMkernel por host para el tráfico de FT. ■ **Tráfico de administración**. Habilita el tráfico de administración del host y vCenter Server. Normalmente, se crea un adaptador de VMkernel de este tipo para los hosts cuando se instala el software ESXi. Es posible crear otro adaptador de VMkernel para el tráfico de administración en el host con la finalidad de proporcionar redundancia. ■ **Tráfico de vSphere Replication**. Controla los datos de replicación salientes que se envían desde el host ESXi de origen al servidor de vSphere Replication. ■ **Tráfico NFC de vSphere Replication**. Controla los datos de replicación entrantes en el sitio de replicación de destino. ■ **vSAN**. Habilita el tráfico de vSAN en el host. Todos los hosts que forman parte de un clúster de vSAN deben tener un adaptador de VMkernel de este tipo.

7 Si ha seleccionado las pilas TCP/IP de vMotion o Aprovisionamiento, haga clic en **Aceptar** en el cuadro de diálogo de advertencia que aparece.

Si ya se ha iniciado una operación de migración activa, esta se ejecuta correctamente incluso después de que se deshabilitan los adaptadores de VMkernel involucrados en la pila de TCP/IP predeterminada de vMotion. Lo mismo ocurre con las operaciones que incluyen adaptadores de VMkernel en la pila de TCP/IP predeterminada que están configurados para tráfico de aprovisionamiento.

8 (opcional) En la página Configuración de IPv4, seleccione una opción para obtener las direcciones IP.

Opción	Descripción
Obtener configuración de IPv4 automáticamente	Use DHCP para obtener la configuración de IP. Debe haber un servidor DHCP presente en la red.
Usar configuración de IPv4 estática	Escriba la dirección IP de IPv4 y la máscara de subred para el adaptador VMkernel. Las direcciones de servidor DNS y puerta de enlace predeterminada de VMkernel para IPv4 se obtienen de la pila TCP/IP seleccionada. Active la casilla **Anular la puerta de enlace predeterminada para este adaptador** e introduzca una dirección de puerta de enlace, en caso de que desee especificar una puerta de enlace diferente para el adaptador de VMkernel.

9 (opcional) En la página Configuración de IPv6, seleccione una opción para obtener las direcciones IPv6.

Opción	Descripción
Obtener las direcciones IPv6 automáticamente por medio de DHCP	Use DHCP para obtener las direcciones IPv6. Debe haber un servidor DHCPv6 presente en la red.
Obtener las direcciones IPv6 automáticamente por medio del anuncio de enrutador	Use el anuncio de enrutador para obtener las direcciones IPv6. En ESXi 6.5 y versiones posteriores, el anuncio de enrutador está habilitado de manera predeterminada, y se admiten las marcas M y O según RFC 4861.
Direcciones IPv6 estáticas	a Haga clic en **Agregar dirección IPv6** para agregar una nueva dirección IPv6. b Introduzca la dirección IPv6 y la longitud del prefijo de subred, y haga clic en **Aceptar**. c Para cambiar la puerta de enlace predeterminada de VMkernel, haga clic en **Anular la puerta de enlace predeterminada para este adaptador**. La dirección de puerta de enlace predeterminada de VMkernel para IPv6 se obtiene de la pila de TCP/IP seleccionada.

10 Revise las selecciones de configuración en la página Listo para finalizar y haga clic en **Finalizar**.

Editar la configuración del adaptador VMkernel

Puede ser necesario modificar el tipo de tráfico admitido para un adaptador VMkernel o la forma en que se obtienen las direcciones IPv4 o IPv6.

Procedimiento

1 En vSphere Web Client, desplácese hasta el host.

2 En la pestañaConfigurar, expanda **Redes** y seleccione **Adaptadores de VMKernel**.

3 Seleccione el adaptador VMkernel que reside en el conmutador distribuido o estándar de destino y, a continuación, haga clic en **Editar**.

4 En la página de propiedades del puerto, seleccione los servicios que desee habilitar.

Casilla	Descripción
Tráfico de vMotion	Permite al adaptador de VMkernel anunciarse a otro host como la conexión de red mediante la cual se envía el tráfico de vMotion. Si esta propiedad no está habilitada para ningún adaptador VMkernel, no es posible la migración con vMotion al host seleccionado.
Tráfico de aprovisionamiento	Controla los datos que se transfieren para una operación de migración de instantáneas, clonación o migración en frío de una máquina virtual.
Tráfico de Fault Tolerance	Permite registrar Fault Tolerance en el host. Solamente se puede usar un adaptador de VMkernel por host para el tráfico de FT.
Tráfico de administración	Habilita el tráfico de administración del host y vCenter Server. Normalmente, se crea un adaptador VMkernel de este tipo para los hosts cuando se instala el software ESXi. Es posible contar con un adaptador VMkernel adicional para el tráfico de administración en el host con la finalidad de proporcionar redundancia.
Tráfico de vSphere Replication	Controla los datos de replicación salientes que se envían desde el host ESXi de origen al servidor de vSphere Replication.
Tráfico NFC de vSphere Replication	Controla los datos de replicación entrantes en el sitio de replicación de destino.
vSAN	Habilita el tráfico de vSAN en el host. Todos los hosts que forman parte de un clúster de vSAN deben tener un adaptador de VMkernel de este tipo.

5 En la página Configuración de NIC, establezca el valor de MTU para el adaptador de red.

6 Con IPv4 habilitado, en la sección de configuración de IPv4, seleccione el método de obtención de direcciones IP.

Opción	Descripción
Obtener configuración de IPv4 automáticamente	Use DHCP para obtener la configuración de IP. Debe haber un servidor DHCP presente en la red.
Usar configuración de IPv4 estática	Escriba la dirección IP de IPv4 y la máscara de subred para el adaptador VMkernel. Las direcciones de servidor DNS y puerta de enlace predeterminada de VMkernel para IPv4 se obtienen de la pila TCP/IP seleccionada. Active la casilla **Anular la puerta de enlace predeterminada para este adaptador** e introduzca una dirección de puerta de enlace, en caso de que desee especificar una puerta de enlace diferente para el adaptador de VMkernel.

7 Con IPv6 habilitado, en la configuración de IPv6, seleccione una opción de obtención de direcciones IPv6.

Nota La opción IPv6 no aparece en los hosts en los que no se ha habilitado IPv6.

Opción	Descripción
Obtener las direcciones IPv6 automáticamente por medio de DHCP	Use DHCP para obtener las direcciones IPv6. Debe haber un servidor DHCPv6 presente en la red.
Obtener las direcciones IPv6 automáticamente por medio del anuncio de enrutador	Use el anuncio de enrutador para obtener las direcciones IPv6. En ESXi 6.5 y versiones posteriores, el anuncio de enrutador está habilitado de manera predeterminada, y se admiten las marcas M y O según RFC 4861.
Direcciones IPv6 estáticas	a Haga clic en **Agregar dirección IPv6** para agregar una nueva dirección IPv6. b Introduzca la dirección IPv6 y la longitud del prefijo de subred, y haga clic en **Aceptar**. c Para cambiar la puerta de enlace predeterminada de VMkernel, haga clic en **Anular la puerta de enlace predeterminada para este adaptador**. La dirección de puerta de enlace predeterminada de VMkernel para IPv6 se obtiene de la pila de TCP/IP seleccionada.

En la página Configuración de IPv6, haga clic en Configuración avanzada para eliminar las direcciones IPv6. Si el anuncio de enrutador está habilitado, es posible que las direcciones eliminadas de este origen vuelvan a aparecer. No está permitido quitar direcciones DHCP en el adaptador VMkernel. Estas direcciones se quitan únicamente cuando la opción DHCP está desactivada.

8 En la página Analizar impacto, compruebe que los cambios aplicados al adaptador de VMkernel no alteren otras operaciones.

9 Haga clic en **Aceptar**.

Anular la puerta de enlace predeterminada de un adaptador de VMkernel

Es posible que necesite anular la puerta de enlace predeterminada de un adaptador de VMkernel para proporcionar otra puerta de enlace para vSphere vMotion.

Cada pila de TCP/IP en un host puede tener una sola puerta de enlace predeterminada. La puerta de enlace predeterminada forma parte de la tabla de enrutamiento y la utilizan todos los servicios que operan en la pila de TCP/IP.

Por ejemplo, los adaptadores vmk0 y vmk1 de VMkernel pueden configurarse en un host.

- vmk0 se utiliza para el tráfico de administración en la subred 10.162.10.0/24, con la puerta de enlace predeterminada 10.162.10.1.
- vmk1 se utiliza para el tráfico de vMotion en la subred 172.16.1.0/24.

Si establece 172.16.1.1 como la puerta de enlace predeterminada para vmk1, vMotion utiliza vmk1 como su interfaz de egreso con la puerta de enlace 172.16.1.1. La puerta de enlace 172.16.1.1 forma parte de la configuración de vmk1 y no se encuentra en la tabla de enrutamiento. Solo los servicios que especifican vmk1 como una interfaz de egreso utilizan esta puerta de enlace. Esto brinda opciones de conectividad adicionales de Capa 3 para servicios que necesitan varias puertas de enlace.

Es posible utilizar vSphere Web Client o un comando ESXCLI para configurar la puerta de enlace predeterminada de un adaptador de VMkernel.

Consulte Crear un adaptador VMkernel en vSphere Standard Switch, Crear un adaptador VMkernel en un host asociado con vSphere Distributed Switch y Configurar la puerta de enlace de un adaptador de VMkernel mediante comandos ESXCLI.

Configurar la puerta de enlace de un adaptador de VMkernel mediante comandos ESXCLI

Puede anular la puerta de enlace predeterminada de un adaptador de VMkernel para proporcionar otra puerta de enlace de vSphere vMotion mediante los comandos ESXCLI.

Procedimiento

1 Abra una conexión de SSH para el host.

2 Inicie sesión como usuario raíz.

3 Ejecute el siguiente comando.

Opción	Descripción
IPv4	`esxcli network ip interface ipv4 set -i vmknic -t static -g IPv4 gateway -I IPv4 address -N mask`

IPv6	**Importante** Debe desactivar la opción DHCPv6 o Anuncio de enrutador para poder configurar la puerta de enlace de vmknic IPv6.
	`esxcli network ip interface ipv6 set -i vmknic -d off -r off`
	Para agregar una dirección IPv6 estática:
	`esxcli network ip interface ipv6 address add -i vmknic -I IPv6 address`
	Para configurar la puerta de enlace de vmknic IPv6:
	`esxcli network ip interface ipv6 set -i vmknic -g IPv6 gateway`

Donde *vmknic* es el nombre del adaptador de VMkernel, *gateway* es la dirección IP de la puerta de enlace, *IP address* es la dirección del adaptador de VMkernel y *mask* es la máscara de red.

Ver la configuración de la pila de TCP/IP en un host

Puede ver la configuración de DNS y de enrutamiento de una pila de TCP/IP en un host. También puede ver las tablas de enrutamiento IPv4 y IPv6, el algoritmo de control de congestión y la cantidad máxima de conexiones permitidas.

Procedimiento

1. En vSphere Web Client, desplácese hasta el host.
2. En la pestaña **Configurar**, expanda **Redes** y seleccione **Configuración de TCP/IP**.
3. Seleccione una pila de la tabla Pilas de TCP/IP.

   Si no hay pilas de TCP/IP personalizadas configuradas en el host, se muestran las pilas de TCP/IP predeterminada, de vMotion y de aprovisionamiento del host.

Resultados

Los detalles de DNS y de enrutamiento sobre la pila de TCP/IP aparecen debajo de la tabla Pilas de TCP/IP. Puede ver las tablas de enrutamiento IPv4 y IPv6 y la configuración de DNS y de enrutamiento de la pila.

Nota La tabla de enrutamiento IPv6 solamente se muestra si IPv6 está habilitado en el host.

La pestaña **Opciones avanzadas** contiene información sobre el algoritmo de control de congestión y la cantidad máxima de conexiones permitidas en la pila.

Cambiar la configuración de una pila de TCP/IP en un host

Puede cambiar la configuración de DNS y de la puerta de enlace predeterminada de una pila de TCP/IP en un host. También puede cambiar el algoritmo de control de congestión, la cantidad máxima de conexiones y el nombre de las pilas de TCP/IP personalizadas.

Nota Solo puede cambiar la configuración de DNS y de la puerta de enlace predeterminada de la pila de TCP/IP predeterminada. No se admite el cambio de la configuración de DNS y de la puerta de enlace predeterminada de pilas de TCP/IP personalizadas.

Procedimiento

1. En vSphere Web Client, desplácese hasta el host.
2. En la pestaña **Configurar**, expanda **Redes** y seleccione **Configuración de TCP/IP**.

3 Seleccione una pila en la tabla, haga clic en **Editar** y realice los cambios que correspondan.

<table>
<tr><th>Página</th><th>Opción</th></tr>
<tr><td>Nombre</td><td>Permite cambiar el nombre de una pila de TCP/IP personalizada.</td></tr>
<tr><td>Configuración de DNS</td><td>Permite seleccionar un método de obtención del servidor DNS.
■ Seleccione Obtener configuración automáticamente de un adaptador de red de VMkernel y seleccione un adaptador de red en el menú desplegable Adaptador de red de VMkernel.
■ Seleccione Introducir configuración manualmente y edite las opciones de configuración de DNS.
a Edite el nombre del host.
b Edite el nombre del dominio.
c Escriba la dirección IP del servidor DNS preferida.
d Escriba una dirección IP del servidor DNS alternativa.
e (opcional) Utilice el cuadro de texto Dominios de búsqueda para especificar los sufijos de DNS que se usarán en la búsqueda de DNS para resolver los nombres de dominio no calificados.</td></tr>
<tr><td>Enrutamiento</td><td>Permite editar la información de la puerta de enlace VMkernel.
Nota Quitar la puerta de enlace predeterminada puede hacer que el cliente pierda conectividad con el host.</td></tr>
<tr><td>Avanzado</td><td>Permite editar la cantidad máxima de conexiones y el algoritmo de control de congestión de la pila.</td></tr>
</table>

4 Haga clic en **Aceptar** para aplicar los cambios.

Pasos siguientes

Se pueden agregar rutas estáticas a puertas de enlace adicionales con comandos de CLI. Para obtener más información, consulte http://kb.vmware.com/kb/2001426

Crear una pila de TCP/IP personalizada

Puede crear una pila de TCP/IP personalizada en un host para reenviar el tráfico de redes a través de una aplicación personalizada.

Procedimiento

1 Abra una conexión de SSH para el host.

2 Inicie sesión como usuario raíz.

3 Ejecute el comando de vSphere CLI.

```
esxcli network ip netstack add -N="stack_name"
```

Resultados

Se crea la pila de TCP/IP personalizada en el host. Puede asignar adaptadores VMkernel a la pila.

Quitar un adaptador VMkernel

Quite un adaptador VMkernel de un conmutador distribuido o estándar de vSphere cuando ya no lo necesite. Asegúrese de dejar al menos un adaptador VMkernel para el tráfico de administración en el host a fin de mantener la conectividad de red.

Procedimiento

1 En vSphere Web Client, desplácese hasta el host.

2 En la pestaña**Configurar**, expanda **Redes** y seleccione **Adaptadores de VMKernel**.

3 Seleccione un adaptador de VMkernel de la lista y haga clic en el icono **Quitar el adaptador de red seleccionado**.

4 En el cuadro de diálogo de confirmación, haga clic en **Analizar impacto**.

5 Si usa adaptadores de iSCSI de software con enlace de puertos, revise el impacto para la configuración de redes.

Opción	Descripción
Sin impacto	iSCSI continuará con su funcionamiento normal después de aplicar la nueva configuración de redes.
Impacto importante	El funcionamiento normal de iSCSI podría interrumpirse si se aplica la nueva configuración de redes.
Impacto crítico	El funcionamiento normal de iSCSI se verá interrumpido si se aplica la nueva configuración de redes.

a Si el impacto en iSCSI es importante o crítico, haga clic en la entrada **iSCSI** y revise los motivos que aparecen en el panel de detalles Análisis.

b Cancele el proceso de quitar el adaptador VMkernel hasta que resuelva las causas de toda reducción crítica o importante de un servicio o, si ningún servicio se ve afectado, cierre el cuadro de diálogo Analizar impacto.

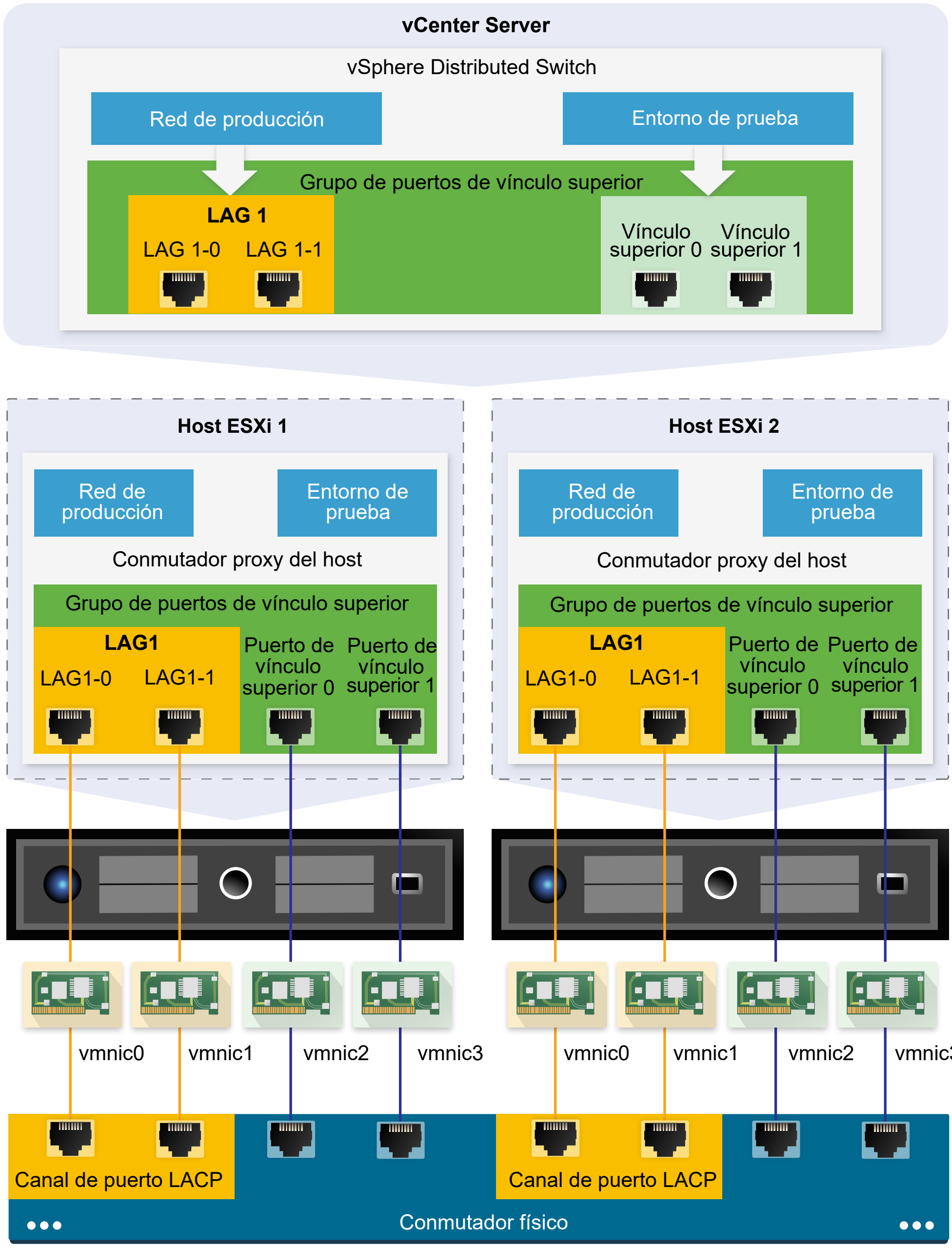
6 Haga clic en **Aceptar**.

Compatibilidad con LACP en vSphere Distributed Switch

5

Cuando la compatibilidad con LACP está habilitada en vSphere Distributed Switch, se pueden conectar hosts ESXi a conmutadores físicos mediante el uso de la adición de enlaces dinámicos. Se pueden crear varios grupos de adición de enlaces (LAG) en un conmutador distribuido para combinar el ancho de banda de NIC físicas en hosts ESXi que están conectados a los canales de puerto LACP.

Figura 5-1. Compatibilidad con LACP mejorada en vSphere Distributed Switch



Configurar LACP en el conmutador distribuido

Se puede configurar un LAG con dos o más puertos y conectar NIC físicas a los puertos. Los puertos de LAG se agrupan en el LAG y la carga del tráfico de red se equilibra entre los puertos a través de un algoritmo de hash de LACP. Se puede utilizar un LAG para controlar el tráfico de los grupos de puertos distribuidos y de ese modo ampliar el ancho de banda de la red, la redundancia y el equilibrio de carga en los grupos de puertos.

Cuando se crea un LAG en un conmutador distribuido, también se crea un objeto de LAG en el conmutador proxy de cada host conectado al conmutador distribuido. Por ejemplo, si se crea un LAG1 con dos puertos, se creará un LAG1 con la misma cantidad de puertos en cada host conectado al conmutador distribuido.

En un conmutador proxy del host, se puede conectar una NIC física a un solo puerto de LAG. En el conmutador distribuido, un solo puerto de LAG puede tener varias NIC físicas de diferentes hosts conectados a él. Las NIC físicas de un host que se conecta a los puertos de LAG deben estar conectadas a los vínculos que participan en un canal de puerto LACP en el conmutador físico.

En un conmutador distribuido, se pueden crear hasta 64 LAG. Un host puede admitir hasta 32 LAG. Sin embargo, la cantidad de LAG que se pueden utilizar depende de la capacidad del entorno físico subyacente y de la topología de la red virtual. Por ejemplo, si el conmutador físico admite hasta cuatro puertos en un canal de puerto LACP, es posible conectar a un LAG hasta cuatro NIC físicas por host.

Configurar canal de puerto en el conmutador físico

Para cada host en el que se desea utilizar LACP, se debe crear un canal de puerto LACP separado en el conmutador físico. Al configurar LACP en el conmutador físico, se deben tener en cuenta los siguientes requisitos:

- La cantidad de puertos en el canal de puerto LACP debe ser igual a la cantidad de NIC físicas que se desean agrupar en el host. Por ejemplo, si se desea combinar el ancho de banda de dos NIC físicas en un host, se debe crear un canal de puerto LACP con dos puertos en el conmutador físico. El LAG en el conmutador distribuido debe estar configurado con al menos dos puertos.
- El algoritmo de hash del canal de puerto LACP en el conmutador físico debe ser el mismo que el algoritmo de hash que está configurado para el LAG en el conmutador distribuido.
- Todas las NIC físicas que se deseen conectar al canal de puerto LACP se deberán configurar con la misma velocidad y dúplex.

Este capítulo incluye los siguientes temas:

- Convertir la compatibilidad con LACP mejorada en vSphere Distributed Switch
- Configurar la formación de equipos y conmutación por error de LACP para grupos de puertos distribuidos
- Configurar un grupo de adición de enlaces para controlar el tráfico de los grupos de puertos distribuidos
- Editar un grupo de adición de enlaces
- Habilitar la compatibilidad con LACP 5.1 en un grupo de puertos de vínculo superior
- Limitaciones de la compatibilidad con LACP en vSphere Distributed Switch

Convertir la compatibilidad con LACP mejorada en vSphere Distributed Switch

Después de actualizar vSphere Distributed Switch de la versión 5.1 a la versión 5.5, 6.0 o 6.5, es posible realizar la conversión a la compatibilidad con LACP mejorada para crear varios LAG en el conmutador distribuido.

Si en el conmutador distribuido existe una configuración de LACP, la mejora de la compatibilidad con LACP crea un nuevo LAG y migra todas las NIC físicas de los vínculos superiores independientes a los puertos de LAG. Para crear una configuración de LACP diferente, debe deshabilitar la compatibilidad con LACP en el grupo de puertos de vínculo superior antes de iniciar la conversión.

Si se produce un error en la conversión a la compatibilidad con LACP mejorada, consulte la *Solución de problemas de vSphere* para obtener información sobre cómo completarla manualmente.

Requisitos previos

- Compruebe que vSphere Distributed Switch sea versión 5.5, 6.0 o 6.5.
- Compruebe que ninguno de los grupos de puertos distribuidos permita que en los puertos individuales se ignore su directiva de formación de equipos de vínculo superior.
- Si convierte desde una configuración LACP existente, compruebe que en el conmutador distribuido haya un solo grupo de puertos de vínculo superior.
- Compruebe que los hosts que participan en el conmutador distribuido estén conectados y respondan.
- Compruebe que tenga el privilegio **Grupo dvPort.Modificar** en los grupos de puertos distribuidos del conmutador.
- Compruebe que en los hosts del conmutador distribuido tenga el privilegio **Host.Configuración.Modificar**.

Nota Cuando actualiza una instancia de vSphere Distributed Switch de la versión 5.1 a la versión 6.5, la compatibilidad con LACP se mejora automáticamente. Si la compatibilidad básica con LACP se habilitó en el conmutador distribuido antes de la actualización, la compatibilidad con LACP debe mejorarse manualmente.

Procedimiento

1. En vSphere Web Client, desplácese hasta el conmutador distribuido.
2. Seleccione **Resumen**.
3. En la sección Características, haga clic en **Mejorar** junto al protocolo Link Aggregation Control Protocol.

4 (opcional) Seleccione **Configuración de exportación** para realizar una copia de seguridad de la configuración del conmutador distribuido y haga clic en **Siguiente**.

La copia de seguridad solo almacena la configuración del conmutador distribuido para vCenter Server. Si se produce un error en la conversión a la compatibilidad con LACP mejorada, es posible utilizar la copia de seguridad para crear un nuevo conmutador distribuido con la misma configuración o realizar la conversión manualmente.

5 Revise los requisitos previos de validación.

Requisitos previos	Descripción
Accesibilidad al grupo de puertos	Posee suficientes privilegios para acceder y modificar el vínculo superior y los grupos de puertos distribuidos en el conmutador.
Configuración de LACP	Tiene un solo grupo de puertos de vínculo superior en el conmutador distribuido.
Anulación de directiva de formación de equipos de vínculo superior	Los grupos de puertos distribuidos no permiten la anulación de su directiva de formación de equipos de vínculo superior en los puertos individuales.
Accesibilidad de hosts	Tiene suficientes privilegios para modificar la configuración de redes de los hosts conectados al conmutador distribuido.
Conectividad de hosts	Los hosts que participan en el conmutador distribuido están conectados y responden.

6 Haga clic en **Siguiente**.

7 Si realiza la conversión desde una configuración de LACP existente, escriba el nombre del nuevo LAG en el campo de texto Nombre.

8 Haga clic en **Siguiente** para revisar los detalles acerca de la conversión y haga clic en **Finalizar**.

Resultados

Convirtió la compatibilidad con LACP mejorada en vSphere Distributed Switch.

Pasos siguientes

Cree varios LAG en el conmutador distribuido para combinar el ancho de banda de varias NIC físicas en los hosts asociados.

Configurar la formación de equipos y conmutación por error de LACP para grupos de puertos distribuidos

Para controlar el tráfico de red de los grupos de puertos distribuidos mediante un LAG, asigne NIC físicas a los puertos de LAG y establezca el LAG como activo en el orden de formación de equipos y conmutación por error de los grupos de puertos distribuidos.

Tabla 5-1. Configuración de formación de equipos y conmutación por error de LACP de los grupos de puertos distribuidos

Orden de conmutación por error	Vínculos superiores	Descripción
activa	Un solo LAG	Puede usar un solo LAG activo o varios vínculos superiores independientes para controlar el tráfico de los grupos de puertos distribuidos. No es posible configurar varios LAG activos ni mezclar LAG activos y vínculos superiores independientes.
En espera	Vacío	No es posible contar con un LAG activo y varios vínculos superiores en espera, ni viceversa. No se admite un LAG y otro LAG en espera.
Sin utilizar	Todos los vínculos superiores independientes y otros LAG (si hubiera)	Dado que solamente puede haber un LAG activo y que la lista En espera debe estar vacía, debe configurar todos los vínculos superiores independientes y otros LAG como sin usar.

Configurar un grupo de adición de enlaces para controlar el tráfico de los grupos de puertos distribuidos

Para combinar el ancho de banda de varias NIC en los hosts, es posible crear un grupo de adición de enlaces (LAG) en el conmutador distribuido y utilizarlo para manejar el tráfico de grupos de puertos distribuidos.

Los LAG recién creados no tienen NIC físicas asignadas a sus puertos y no se utilizan en el orden de formación de equipos y conmutación por error de los grupos de puertos distribuidos. Para manejar el tráfico de red de los grupos de puertos distribuidos mediante el uso de un LAG, es necesario migrar el tráfico desde los vínculos superiores independientes hacia el LAG.

Requisitos previos

- Compruebe que en cada host en el que desea utilizar LACP exista un canal de puerto LACP separado en el conmutador físico. Consulte Capítulo 5 Compatibilidad con LACP en vSphere Distributed Switch.
- Compruebe que vSphere Distributed Switch en el que se configura el LAG tenga la versión 5.5 o 6.0.
- Compruebe que el conmutador distribuido admita el LACP mejorado.

Procedimiento

1 Crear un grupo de adición de enlaces

Para migrar el tráfico de red de los grupos de puertos distribuidos a un grupo de adición de enlaces (LAG), es necesario crear un nuevo LAG en el conmutador distribuido.

2 Configurar un grupo de adición de enlaces en espera en el orden de formación de equipos y conmutación por error de los grupos de puertos distribuidos

El nuevo grupo de adición de enlaces (LAG) no se utiliza de forma predeterminada en el orden de formación de equipos y conmutación por error de los grupos de puertos distribuidos. Dado que solo un LAG o los vínculos superiores independientes pueden estar activos en los grupos de puertos distribuidos, se debe crear una configuración intermedia de formación de equipos y conmutación por error, donde el LAG permanece en espera. Esta configuración permite migrar NIC físicas a los puertos de LAG y mantener activada la conectividad de red.

3 Asignar NIC físicas a los puertos del grupo de adición de enlaces

Estableció el nuevo grupo de adición de enlaces (LAG) en el modo en espera para el orden de formación de equipos y conmutación por error de los grupos de puertos distribuidos. Configurar el LAG en espera permite migrar sin inconvenientes las NIC físicas de los vínculos superiores independientes a los puertos de LAG sin perder la conectividad de red.

4 Configurar grupo de adición de enlaces como activo en el orden de formación de equipos y conmutación por error del grupo de puertos distribuidos

Migró las NIC físicas a los puertos del grupo de adición de enlaces (LAG). Establezca el LAG como activo y transfiera todos los vínculos superiores independientes como vínculos sin utilizar en el orden de formación de equipos y conmutación por error de los grupos de puertos distribuidos.

Crear un grupo de adición de enlaces

Para migrar el tráfico de red de los grupos de puertos distribuidos a un grupo de adición de enlaces (LAG), es necesario crear un nuevo LAG en el conmutador distribuido.

Procedimiento

1 En vSphere Web Client, desplácese hasta el conmutador distribuido.

2 En la pestaña **Configurar**, expanda **Configuración** y seleccione **LACP**.

3 Haga clic en el icono **Nuevo grupo de adición de enlaces**.

4 Asígnele un nombre al nuevo LAG.

5 Establezca la cantidad de puertos para el LAG.

Establezca la misma cantidad de puertos para el LAG que la cantidad de puertos en el canal de puerto LACP del conmutador físico. Un puerto de un LAG cumple la misma función que un vínculo superior en el conmutador distribuido. Todos los puertos de LAG forman un equipo NIC en el contexto del LAG.

6 Seleccione el modo de negociación LACP del LAG.

Opción	Descripción
activa	Todos los puertos de LAG están en modo de negociación activa. Los puertos de LAG inician negociaciones con el canal de puerto LACP en el conmutador físico mediante el envío de paquetes LACP.
Pasiva	Los puertos de LAG están en modo de negociación pasiva. Responden a los paquetes LACP que reciben, pero no inician una negociación LACP.

Si los puertos habilitados para LACP en el conmutador físico están en modo de negociación activa, es posible establecer los puertos de LAG en modo pasivo, y viceversa.

7 Seleccione un modo de equilibrio de carga desde los algoritmos de hash que define LACP.

Nota El algoritmo de hash debe ser el mismo que el algoritmo de hash que se establece en el canal de puerto LACP del conmutador físico.

8 Establezca las directivas de NetFlow y VLAN para el LAG.

Esta opción está activa cuando la anulación de las directivas de VLAN y NetFlow por puerto de vínculo superior individual está habilitada en el grupo de puertos de vínculo superior. Si establece las directivas de VLAN y NetFlow para el LAG, estas anularán las directivas establecidas en el nivel del grupo de puertos de vínculo superior.

9 Haga clic en **Aceptar**.

Resultados

El nuevo LAG no se utiliza en el orden de formación de equipos y conmutación por error de los grupos de puertos distribuidos. No se han asignado NIC físicas a los puertos de LAG.

Como sucede con los vínculos superiores independientes, el LAG tiene una representación en cada host que está asociada con el conmutador distribuido. Por ejemplo, si se crea un LAG1 con dos puertos en el conmutador distribuido, en cada host que está asociado con el conmutador distribuido se crea un LAG1 con dos puertos.

Pasos siguientes

Establezca el LAG en modo de espera en la configuración de formación de equipos y conmutación por error de los grupos de puertos distribuidos. De esta manera, se crea una configuración intermedia que permite migrar el tráfico de red al LAG sin perder la conectividad de red.

Configurar un grupo de adición de enlaces en espera en el orden de formación de equipos y conmutación por error de los grupos de puertos distribuidos

El nuevo grupo de adición de enlaces (LAG) no se utiliza de forma predeterminada en el orden de formación de equipos y conmutación por error de los grupos de puertos distribuidos. Dado que solo un LAG o los vínculos superiores independientes pueden estar activos en los grupos de puertos distribuidos, se debe crear una configuración intermedia de formación de equipos y

conmutación por error, donde el LAG permanece en espera. Esta configuración permite migrar NIC físicas a los puertos de LAG y mantener activada la conectividad de red.

Procedimiento

1 Desplácese hasta el conmutador distribuido.
2 En el menú **Acciones** seleccione **Grupo de puertos distribuidos > Administrar grupos de puertos distribuidos**.
3 Seleccione **Formación de equipos y conmutación por error** y haga clic en **Siguiente**.
4 Seleccione los grupos de puertos donde desea utilizar el LAG.
5 En el orden de conmutación por error, seleccione el LAG y utilice la flecha hacia arriba para moverlo a la lista de vínculos superiores en espera.
6 Haga clic en **Siguiente**, revise el mensaje que informa sobre el uso de la configuración intermedia de formación de equipos y conmutación por error, y haga clic en **Aceptar**.
7 En la página Listo para finalizar, haga clic en **Finalizar**.

Pasos siguientes

Migre las NIC físicas desde los vínculos superiores en espera hacia los puertos de LAG.

Asignar NIC físicas a los puertos del grupo de adición de enlaces

Estableció el nuevo grupo de adición de enlaces (LAG) en el modo en espera para el orden de formación de equipos y conmutación por error de los grupos de puertos distribuidos. Configurar el LAG en espera permite migrar sin inconvenientes las NIC físicas de los vínculos superiores independientes a los puertos de LAG sin perder la conectividad de red.

Requisitos previos

- Compruebe que todos los puertos de LAG o los puertos con LACP correspondientes del conmutador físico estén en el modo de negociación de LACP activo.
- Compruebe que las NIC físicas que desee asignar a los puertos de LAG tengan la misma velocidad y estén configuradas con el modo dúplex completo.

Procedimiento

1 En vSphere Web Client, desplácese hasta el conmutador distribuido donde reside el LAG.
2 En el menú **Acciones**, seleccione **Agregar y administrar hosts**.
3 Seleccione **Administrar redes de host**.
4 Seleccione el host cuyas NIC físicas desee asignar a los puertos de LAG y haga clic en **Siguiente**.
5 En la página Seleccionar tareas de adaptador de red, seleccione **Administrar adaptadores físicos** y haga clic en **Siguiente**.

6 En la página Administrar adaptadores de red físicos, seleccione una NIC y haga clic en **Asignar un vínculo superior**.

7 Seleccione un puerto de LAG y haga clic en **Aceptar**.

8 Repita los procesos del Paso 6 y Paso 7 para todas las NIC físicas que desee asignar a los puertos de LAG.

9 Finalice el asistente.

Ejemplo: Configurar dos NIC físicas para un LAG en el asistente Agregar y administrar hosts

Por ejemplo, si hay un LAG con dos puertos, configure una NIC física en cada puerto de LAG mediante el asistente **Agregar y administrar hosts**.

Pasos siguientes

Establezca el LAG como activo y transfiera los vínculos superiores independientes a vínculos sin utilizar en el orden de formación de equipos y conmutación por error de los grupos de puertos distribuidos.

Configurar grupo de adición de enlaces como activo en el orden de formación de equipos y conmutación por error del grupo de puertos distribuidos

Migró las NIC físicas a los puertos del grupo de adición de enlaces (LAG). Establezca el LAG como activo y transfiera todos los vínculos superiores independientes como vínculos sin utilizar en el orden de formación de equipos y conmutación por error de los grupos de puertos distribuidos.

Procedimiento

1 Desplácese hasta el conmutador distribuido.

2 En el menú **Acciones** seleccione **Grupo de puertos distribuidos > Administrar grupos de puertos distribuidos**.

3 Seleccione **Formación de equipos y conmutación por error** y haga clic en **Siguiente**.

4 Seleccione los grupos de puertos donde establece el LAG en espera y haga clic en **Siguiente**.

5 En Orden de conmutación por error, utilice las flechas hacia arriba y hacia abajo para desplazar el LAG en la lista Activos, todos los vínculos superiores independientes en la lista Sin utilizar y dejar vacía la lista En espera.

6 Haga clic en **Siguiente** y, a continuación, en **Finalizar**.

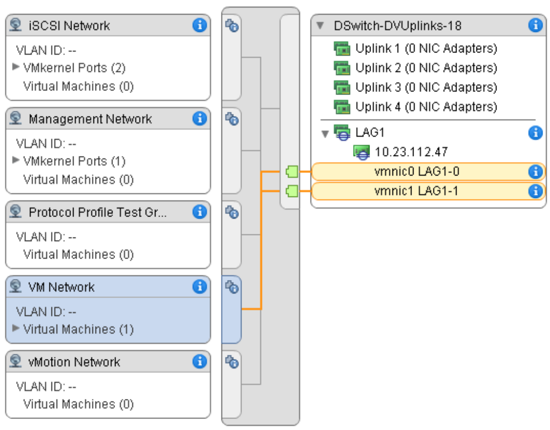
Resultados

Migró correctamente el tráfico de red de los vínculos superiores independientes a un LAG para grupos de puertos distribuidos y creó una configuración de formación de equipos y conmutación por error de LACP para los grupos.

Ejemplo: Topología de un conmutador distribuido que utiliza un LAG

Si configura un LAG con dos puertos para controlar el tráfico de un grupo de puertos distribuidos, puede comprobar la topología del conmutador distribuido para ver cómo cambió a partir de la nueva configuración.

Figura 5-2. Topología de conmutador distribuido con un LAG



Editar un grupo de adición de enlaces

Edite la configuración de un grupo de adición de enlaces (LAG) si necesita combinar más puertos al grupo o modificar el modo de negociación de LACP, el algoritmo de equilibrio de carga o las directivas de VLAN y NetFlow.

Procedimiento

1 En vSphere Web Client, desplácese hasta vSphere Distributed Switch.

2 En la pestaña **Configurar**, expanda **Configuración** y seleccione **LACP**.

3 Haga clic en el icono **Nuevo grupo de adición de enlaces**.

4 En el cuadro de texto **Nombre**, escriba un nuevo nombre para el LAG.

5 Cambie la cantidad de puertos del LAG si desea agregar más NIC físicas.

   Las nuevas NIC deben estar conectadas a puertos que formen parte de un canal de puerto LACP en el conmutador físico.

6 Cambie el modo de negociación de LACP del LAG.

   Si todos los puertos del canal de puerto LACP físico están en el modo de LACP activo, puede cambiar el LAG a un modo pasivo y viceversa.

7 Cambie el modo de equilibrio de carga del LAG.

   Puede seleccionar uno de los algoritmos de equilibrio de carga que define LACP.

8 Cambie las directivas de VLAN y de NetFlow.

Esta opción está activa cuando la opción para anular las directivas de VLAN y NetFlow de puertos individuales está habilitada en el grupo de puertos de vínculo superior. Si modifica las directivas de VLAN y NetFlow del LAG, se anulan las directivas establecidas en el nivel de grupo de puertos de vínculo superior.

9 Haga clic en **Aceptar**.

Habilitar la compatibilidad con LACP 5.1 en un grupo de puertos de vínculo superior

Se puede habilitar la compatibilidad con LACP en un grupo de puertos de vínculo superior para vSphere Distributed Switches 5.1 y para los conmutadores actualizados a la versión 5.5 o 6.0 que no tienen la compatibilidad con LACP mejorada.

Requisitos previos

- Compruebe que por cada host en el que desea utilizar LACP exista un canal de puerto LACP separado en el conmutador físico.
- Compruebe que los grupos de puertos distribuidos tengan su directiva de equilibrio de carga establecida en el hash de IP.
- Compruebe que el canal de puerto LACP en el conmutador físico esté configurado con el equilibrio de carga según el hash de IP.
- Compruebe que los grupos de puertos distribuidos tengan una directiva de detección de error de red establecida solamente en estado de vínculo.
- Compruebe que los grupos de puertos distribuidos tienen todos los vínculos superiores establecidos como activos en su orden de formación de equipos y conmutación por error.
- Compruebe que todas las NIC físicas que estén conectadas a los vínculos superiores tengan la misma velocidad y estén configuradas en dúplex completo.

Procedimiento

1 En vSphere Web Client, desplácese hasta un grupo de puertos de vínculo superior.

   a Seleccione un conmutador distribuido y haga clic en la pestaña **Redes**.

   b Haga clic en **Grupos de puertos de vínculo superior** y seleccione el grupo de puertos de vínculo superior.

2 Haga clic en la pestaña **Configurar** y seleccione **Propiedades**.

3 Haga clic en **Editar**.

4 En la sección LACP, utilice la lista desplegable para habilitar LACP.

5 Establezca el modo de negociación de LACP del grupo de puertos de vínculo superior.

Opción	Descripción
Activa	Todos los puertos de vínculo superior en el grupo están en modo de negociación activa. Los puertos de vínculo superior inician negociaciones con los puertos habilitados para LACP en el conmutador físico mediante el envío de paquetes de LACP.
Pasiva	Todos los puertos de vínculo superior están en modo de negociación pasiva. Responden a los paquetes de LACP que reciben, pero no inician la negociación de LACP.

Si los puertos habilitados para LACP en el conmutador físico están en modo de negociación activa, los puertos de vínculo superior se pueden establecer en modo pasivo y viceversa.

6 Haga clic en **Aceptar**.

Limitaciones de la compatibilidad con LACP en vSphere Distributed Switch

La compatibilidad con LACP en una instancia de vSphere Distributed Switch permite a los dispositivos de red negociar el agrupamiento automático de vínculos al enviar paquetes de LACP a un elemento del mismo nivel. Sin embargo, la compatibilidad con LACP en vSphere Distributed Switch presenta limitaciones.

- LACP no es compatible con el enlace de puertos de iSCSI de software. Si no se utiliza el enlace de puertos, se admiten múltiples rutas de iSCSI a través de LAG.
- La configuración de la compatibilidad con LACP no está disponible en los perfiles de host.
- La compatibilidad con LACP no es posible entre los hosts ESXi anidados.
- La compatibilidad con LACP no funciona con ESXi Dump Collector.
- Los paquetes de control LACP (LACPDU) no se reflejan cuando se habilita la creación de reflejo del puerto.
- La comprobación de estado de formación de equipos y conmutación por error no funciona en los puertos de LAG. LACP comprueba la conectividad de los puertos de LAG.
- La compatibilidad con LACP mejorada funciona correctamente cuando solo un LAG maneja el tráfico por puerto distribuido o por grupo de puertos.
- La compatibilidad con LACP 5.1 solo funciona con el equilibrio de carga según el hash de IP y con la detección de conmutación por error de red de estado de vínculos.
- La compatibilidad con LACP 5.1 proporciona un solo LAG por conmutador distribuido y por host.

Hacer una copia de seguridad y restaurar la configuración de redes

6

vSphere 5.1 y posteriores permiten hacer copias de seguridad y restaurar la configuración de vSphere Distributed Switch, además de grupos de puertos distribuidos y de grupos de puertos de vínculo superior en el caso de cambios no válidos o de una transferencia a otra implementación.

Este capítulo incluye los siguientes temas:

- Hacer una copia de seguridad y restaurar una configuración de vSphere Distributed Switch
- Exportar, importar y restaurar la configuración del grupo de puertos distribuidos de vSphere

Hacer una copia de seguridad y restaurar una configuración de vSphere Distributed Switch

vCenter Server ofrece la capacidad de hacer copias de seguridad y restaurar la configuración de vSphere Distributed Switch. Puede restaurar la configuración de la red virtual en caso de un error en la base de datos o en una actualización. También puede utilizar una configuración de conmutador guardada como plantilla para crear una copia del conmutador en el mismo entorno de vSphere o en uno nuevo.

Puede importar o exportar la configuración de un conmutador distribuido, incluidos sus grupos de puertos. Para obtener información sobre cómo exportar, importar y restaurar la configuración de un grupo de puertos, consulte Exportar, importar y restaurar la configuración del grupo de puertos distribuidos de vSphere.

Nota Puede usar un archivo de configuración almacenado para restaurar las asociaciones de directivas y hosts en el conmutador distribuido. No es posible restaurar la conexión de las NIC físicas con los puertos del vínculo superior o con los puertos de grupos de agregación de vínculos.

Exportar la configuración de vSphere Distributed Switch

Puede exportar la configuración de vSphere Distributed Switch y de un grupo de puertos distribuidos a un archivo. El archivo conserva la configuración de red válida y permite transferirla a otros entornos.

Esta funcionalidad está disponible exclusivamente con vCenter Server 5.1 y versiones posteriores.

Puede exportar la configuración de un conmutador antes de actualizar vCenter Server si actualiza desde vCenter Server 5.1. Si actualiza vCenter Server desde una versión anterior a 5.1, haga una copia de seguridad de la configuración del conmutador antes de actualizar vCenter Server a la versión 6.0.

Requisitos previos

Compruebe que la versión de vCenter Server sea 5.1 o una versión posterior.

Procedimiento

1 En vSphere Web Client, desplácese hasta el conmutador distribuido.

2 Haga clic con el botón derecho en el conmutador distribuido y seleccione **Configuración > Exportar configuración**.

3 Seleccione si desea exportar la configuración del conmutador distribuido o exportar la configuración del conmutador distribuido y todos los grupos de puertos.

4 (opcional) Puede escribir notas sobre la configuración en el campo **Descripciones**.

5 Haga clic en **Aceptar**.

6 Haga clic en **Sí** para guardar el archivo de configuración en el sistema local.

Pasos siguientes

Puede utilizar el archivo de configuración exportado para las siguientes tareas:

- Crear una copia del conmutador distribuido exportado en un entorno de vSphere. Consulte Importar la configuración de vSphere Distributed Switch.
- Sobrescribir la configuración de un conmutador distribuido existente. Consulte Restaurar una configuración de vSphere Distributed Switch.

También puede exportar, importar y restaurar únicamente la configuración del grupo de puertos. Consulte Exportar, importar y restaurar la configuración del grupo de puertos distribuidos de vSphere.

Importar la configuración de vSphere Distributed Switch

Importe un archivo de configuración almacenado para crear un nuevo vSphere Distributed Switch o para restaurar un conmutador que se eliminó antes.

En vSphere 5.1 y posteriores, es posible importar un conmutador distribuido con vSphere Web Client.

El archivo de configuración contiene la configuración de redes del conmutador. Mediante su uso, también se puede replicar el conmutador en otros entornos virtuales.

Nota Se puede utilizar un archivo de configuración guardado para replicar la instancia del conmutador, sus asociaciones de host y las directivas. No se puede replicar la conexión de las NIC físicas con puertos de vínculo superior o con puertos en grupos de adición de enlaces.

Requisitos previos

Compruebe que la versión de vCenter Server sea 5.1.0 y posteriores.

Procedimiento

1 En vSphere Web Client, desplácese hasta un centro de datos.

2 Haga clic con el botón derecho en el centro de datos y seleccione **Conmutador distribuido > Importar conmutador distribuido**.

3 Desplácese hasta la ubicación del archivo de configuración.

4 Para asignar las claves del archivo de configuración para el conmutador y sus grupos de puertos, active la casilla **Mantener identificadores originales del grupo de puertos y del conmutador distribuido** y haga clic en **Siguiente**.

   Puede utilizar la opción **Mantener identificadores originales del grupo de puertos y del conmutador distribuido** en los siguientes casos:

   - Volver a crear un conmutador eliminado.
   - Restaurar un conmutador cuya actualización tuvo un error.

   Todos los grupos de puertos se vuelven a crear y los hosts que estuvieron conectados al conmutador se agregan de nuevo.

5 Revise la configuración del conmutador y haga clic en **Finalizar**.

Resultados

Se crea un nuevo conmutador distribuido con la configuración del archivo de configuración. Si se incluye información sobre el grupo de puertos distribuidos en el archivo de configuración, también se crean los grupos de puertos.

Restaurar una configuración de vSphere Distributed Switch

Utilice la opción de restauración para restablecer la configuración de un conmutador distribuido existente a las opciones del archivo de configuración. Al restaurar un conmutador distribuido, se cambia la configuración del conmutador seleccionado por las opciones guardadas en el archivo de configuración.

Nota Puede usar un archivo de configuración almacenado para restaurar las asociaciones de directivas y hosts en el conmutador distribuido. No es posible restaurar la conexión de las NIC físicas con los puertos del vínculo superior o con los puertos de grupos de agregación de vínculos.

Requisitos previos

Compruebe que la versión de vCenter Server sea 5.1 o una versión posterior.

Procedimiento

1 En vSphere Web Client, desplácese hasta el conmutador distribuido.

2 En el navegador, haga clic con el botón derecho en el conmutador distribuido y seleccione **Configuración > Restaurar configuración**.

3 Busque el archivo de copia de seguridad de configuración que desea utilizar.

4 Seleccione **Restaurar conmutador distribuido y todos los grupos de puertos** o **Restaurar solo conmutador distribuido** y haga clic en **Siguiente**.

5 Revise el resumen de información de la restauración.

   Si restaura un conmutador distribuido, se sobrescribe la configuración actual del conmutador distribuido y de sus grupos de puertos. No se eliminan los grupos de puertos existentes que no formen parte del archivo de configuración.

6 Haga clic en **Finalizar**.

   La configuración del conmutador distribuido se restauró a las opciones del archivo de configuración.

Exportar, importar y restaurar la configuración del grupo de puertos distribuidos de vSphere

Puede exportar la configuración de un grupo de puertos distribuidos de vSphere a un archivo. El archivo de configuración permite conservar la configuración válida del grupo de puertos y utilizarla en otras implementaciones.

Puede exportar la información del grupo de puertos al mismo tiempo que exporta la configuración de conmutadores distribuidos. Consulte Hacer una copia de seguridad y restaurar una configuración de vSphere Distributed Switch.

Exportar la configuración de un grupo de puertos distribuidos de vSphere

Es posible exportar en un archivo la configuración de un grupo de puertos distribuidos. La configuración conserva los valores de red válidos, lo que habilita la distribución de estos valores a otras implementaciones.

Esta funcionalidad solo está disponible con vSphere Web Client 5.1 o posterior. Sin embargo, puede exportar la configuración de cualquier versión de un puerto distribuido si utiliza vSphere Web Client 5.1 o posterior.

Procedimiento

1 Busque un grupo de puertos distribuidos en vSphere Web Client.

   a Seleccione un conmutador distribuido y haga clic en la pestaña **Redes**.

   b Haga clic en **Grupos de puertos distribuidos**.

2 Haga clic con el botón derecho en el grupo de puertos distribuidos y seleccione **Exportar configuración**.

3 (opcional) En el campo **Descripciones** escriba notas acerca de esta configuración.

4 Haga clic en **Aceptar**.

   Haga clic en **Sí** para guardar el archivo de configuración en el sistema local.

Resultados

Ahora tiene un archivo de configuración que contiene toda la configuración correspondiente al grupo de puertos distribuidos seleccionado. Puede utilizar este archivo para crear varias copias de esta configuración en una implementación existente o sobrescribir la configuración de grupos de puertos distribuidos existentes para cumplir con la configuración seleccionada.

Pasos siguientes

Puede utilizar el archivo de configuración exportado para realizar las siguientes tareas:

- Para crear una copia del grupo de puertos distribuidos exportado, consulte Importar una configuración de grupo de puertos distribuidos de vSphere.
- Para sobrescribir la configuración de un grupo de puertos distribuidos existente, consulte Restaurar una configuración del grupo de puertos distribuidos de vSphere.

Importar una configuración de grupo de puertos distribuidos de vSphere

Utilice la importación para crear un grupo de puertos distribuidos desde un archivo de configuración.

Si un grupo de puertos existente tiene el mismo nombre que le grupo de puertos importado, se agregará un número entre paréntesis al nuevo nombre del grupo de puertos. Las opciones de la configuración importada se aplicarán al nuevo grupo de puertos, y la configuración del grupo de puertos original no cambiará.

Esta funcionalidad solo está disponible con vSphere Web Client 5.1 o posterior. Sin embargo, se puede exportar la configuración de cualquier versión de un puerto distribuido si se utiliza vSphere Web Client 5.1 y posterior.

Procedimiento

1 En vSphere Web Client, desplácese hasta el conmutador distribuido.

2 Haga clic con el botón derecho en el conmutador distribuido y seleccione **Grupo de puertos distribuidos > Importar grupo de puertos distribuidos**.

3 Desplácese hasta la ubicación del archivo de configuración guardado y haga clic en **Siguiente**.

4 Revise la configuración de importación antes de completar la importación.

5 Haga clic en **Finalizar**.

Restaurar una configuración del grupo de puertos distribuidos de vSphere

Utilice la opción de restauración para restablecer la configuración de un grupo de puertos distribuidos existente a las opciones de un archivo de configuración.

Esta funcionalidad solo está disponible con vSphere Web Client 5.1 o posterior. Sin embargo, se puede restaurar la configuración desde cualquier versión de un conmutador distribuido si se utiliza vSphere Web Client 5.1 o posterior.

Procedimiento

1 Busque un grupo de puertos distribuidos en vSphere Web Client.

   a Seleccione un conmutador distribuido y haga clic en la pestaña **Redes**.

   b Haga clic en **Grupos de puertos distribuidos**.

2 Haga clic con el botón derecho en el grupo de puertos distribuidos y seleccione **Restaurar configuración**.

3 Seleccione una de las siguientes opciones y haga clic en **Siguiente**:

   - **Restaurar a una configuración previa** para revertir la configuración del grupo de puertos al paso anterior. Si ha ejecutado más de un paso de configuración, no puede hacer una restauración total del grupo de puertos.
   - **Restaurar configuración desde un archivo** permite restaurar la configuración del grupo de puertos desde un archivo de copia de seguridad exportado. También puede utilizar un archivo de copia de seguridad de conmutador distribuido, siempre que contenga información sobre la configuración del grupo de puertos.

4 Revise el resumen de información de la restauración.

   La operación de restauración sobrescribe la configuración actual del grupo de puertos distribuidos con las opciones de la copia de seguridad. Si está restaurando la configuración del grupo de puertos desde un archivo de copia de seguridad de un conmutador, la operación de restauración no elimina los grupos de puertos existentes que no formen parte del archivo.

5 Haga clic en **Finalizar**.

Revertir y recuperar la red de administración

7

En vSphere 5.1 y versiones posteriores, puede impedir y recuperar los errores de configuración de la red de administración gracias a las funciones de reversión y recuperación de vSphere Distributed Switch y vSphere Standard Switch.

La reversión está disponible para los conmutadores estándar y distribuidos. Para reparar una configuración no válida de la red de administración, puede establecer una conexión directa a un host a fin de solucionar los problemas a través de la DCUI.

Este capítulo incluye los siguientes temas:

Revertir redes de vSphere

Cuando se revierten los cambios de configuración, vSphere impide que los hosts pierdan la conexión con vCenter Server debido a un error de configuración de la red de administración.

En vSphere 5.1 y versiones posteriores, la reversión de redes está habilitada de forma predeterminada. Sin embargo, puede habilitar o deshabilitar las reversiones en el nivel de vCenter Server.

Reversiones de redes del host

Las reversiones de red del host se producen cuando se hace un cambio no válido en la configuración de redes para la conexión con vCenter Server. Los cambios de red que desconectan un host también activan una reversión. Algunos ejemplos de cambios de la configuración de redes del host que podrían activar una reversión:

- Actualización de la velocidad o la función dúplex de una NIC física.
- Actualización de la configuración de DNS y de enrutamiento.
- Actualización de las directivas de formación de equipos y conmutación por error o de las directivas de catalogación de tráfico de un grupo de puertos estándar que contenga el adaptador de red VMkernel de administración.

- Actualización de la VLAN de un grupo de puertos estándar que contenga el adaptador de red VMkernel de administración.
- Aumento del valor de MTU del adaptador de red VMkernel de administración y su conmutador a un valor no admitido por la infraestructura física.
- Cambio de la configuración de IP de los adaptadores de red VMkernel de administración.
- Quitar el adaptador de red VMkernel de administración de un conmutador estándar o distribuido.
- Quitar una NIC física de un conmutador estándar o distribuido que contenga el adaptador de red VMkernel de administración.
- Migrar el adaptador VMkernel de administración de un conmutador estándar a un conmutador distribuido de vSphere.

Si una red se desconecta por alguna de estas razones, se produce un error en la tarea y el host se revierte a la última configuración válida.

Reversiones de vSphere Distributed Switch

Las reversiones del conmutador distribuido se ejecutan cuando se hacen actualizaciones no válidas de los conmutadores distribuidos, los grupos de puertos distribuidos o los puertos distribuidos. Los siguientes cambios de la configuración de un conmutador distribuido activan una reversión:

- Cambio del valor de MTU de un conmutador distribuido.
- Cambio de las siguientes opciones del grupo de puertos distribuidos del adaptador de red VMkernel de administración:
  - Formación de equipos y conmutación por error
  - VLAN
  - Catalogación de tráfico
- Bloqueo de todos los puertos del grupo de puertos distribuidos que contenga el adaptador de red VMkernel de administración.
- Anulación de las directivas en el nivel del puerto distribuido del adaptador de red VMkernel de administración.

Si una configuración deja de tener validez debido a alguno de los cambios, es posible que uno o varios hosts queden desincronizados con el conmutador distribuido.

Si sabe dónde se encuentra la opción de configuración en conflicto, puede corregirla manualmente. Por ejemplo, si migró un adaptador de red VMkernel de administración a una VLAN nueva, es posible que la VLAN no haya establecido el tronco en el conmutador físico. Si corrige la configuración del conmutador físico, la siguiente sincronización de conmutador distribuido a host resolverá el problema.

Si no sabe con certeza dónde se encuentra el problema, puede restaurar el estado del conmutador distribuido o el grupo de puertos distribuidos a una configuración anterior. Consulte Restaurar una configuración del grupo de puertos distribuidos de vSphere.

Deshabilitar la reversión de redes

En vSphere 5.1 y versiones posteriores, la reversión está habilitada de forma predeterminada. Puede deshabilitar la reversión en vCenter Server mediante vSphere Web Client.

Procedimiento

1 En vSphere Web Client, desplácese hasta una instancia de vCenter Server.

2 En la pestaña **Configurar**, expanda **Configuración** y seleccione **Configuración avanzada**.

3 Haga clic en **Editar**.

4 Seleccione la clave `config.vpxd.network.rollback` y cambie el valor a false.

   Si la clave no está presente, puede agregarla y establecer el valor en false.

5 Haga clic en **Aceptar**.

6 Reinicie vCenter Server para aplicar los cambios.

Deshabilitar la reversión de red mediante el archivo de configuración de vCenter Server

En vSphere 5.1 y versiones posteriores, la reversión está habilitada de forma predeterminada. Para deshabilitar la reversión, puede editar el archivo de configuración `vpxd.cfg` de vCenter Server directamente.

Procedimiento

1 En el equipo host de vCenter Server, desplácese hasta el directorio que contiene el archivo de configuración:

   - En un sistema operativo Windows Server, la ubicación del directorio es `C:\ProgramData\VMware\CIS\cfg\vmware-vpx`.
   - En vCenter Server Appliance, la ubicación del directorio es `/etc/vmware-vpx`.

2 Abra el archivo `vpxd.cfg` para editarlo.

3 En el elemento `<network>`, establezca el elemento `<rollback>` en **`false`**:

```
<config>
 <vpxd>
  <network>
    <rollback>false</rollback>
  </network>
 </vpxd>
</config>
```

4 Guarde y cierre el archivo.

5 Reinicie el sistema vCenter Server.

Solucionar errores en la configuración de la red de administración en vSphere Distributed Switch

En vSphere 5.1 y versiones posteriores, es posible utilizar la interfaz de usuario de la consola directa (DCUI) para restaurar la conexión entre vCenter Server y un host que accede a la red de administración a través de un conmutador distribuido.

Si la reversión de redes está deshabilitada, una configuración errónea del grupo de puertos correspondiente a la red de administración del conmutador distribuido ocasionará que se pierda conexión entre vCenter Server y los hosts que se agregan al conmutador. Es necesario utilizar la DCUI para conectar individualmente cada host.

Si los adaptadores VMkernel que manejan otros tipos de tráfico (vMotion, Fault Tolerance, etc.) utilizan los mismos vínculos superiores que usted utiliza para restaurar la red de administración, los adaptadores perderán conectividad de red después de la restauración.

Para obtener más información sobre cómo acceder a la DCUI y utilizarla, consulte la documentación de *Seguridad de vSphere*.

Nota La recuperación de la conexión de administración en un conmutador distribuido no es compatible con instancias de ESXi sin estado.

Requisitos previos

Compruebe que la red de administración se configura en un grupo de puertos en el conmutador distribuido.

Procedimiento

1 Conéctese a la DCUI del host.

2 En el menú **Opciones de restauración de red**, seleccione **Restaurar vDS**.

3 Configure los vínculos superiores y opcionalmente la VLAN para la red de administración.

4 Aplique la configuración.

Resultados

La DCUI crea un puerto local efímero y aplica los valores provistos para la VLAN y los vínculos superiores. La DCUI mueve el adaptador VMkernel para la red de administración al nuevo puerto local para restaurar la conectividad con vCenter Server.

Pasos siguientes

Después de que se restablezca la conexión del host a vCenter Server, corrija la configuración del grupo de puertos distribuidos y vuelva a agregar el adaptador VMkernel al grupo.

Directivas de redes 8

Las directivas establecidas en el nivel del conmutador estándar o del grupo de puertos distribuidos se aplican a todos los grupos de puertos en el conmutador estándar o a puertos en el grupo de puertos distribuidos. Las excepciones son las opciones de configuración que se anulan en el nivel del grupo de puertos estándar o del grupo de puertos distribuidos.

Vea el vídeo sobre la aplicación de directivas de redes en los conmutadores estándar y distribuidos de vSphere.

Trabajar con directivas de redes (https://vmwaretv.vmware.com/media/t/1_0bjobp2b)

- Aplicar directivas de redes en vSphere Standard Switch o vSphere Distributed Switch

  En vSphere Standard Switch y vSphere Distributed Switch se aplican directivas de redes diferentes. Algunas de las directivas disponibles para vSphere Distributed Switch no lo están para vSphere Standard Switch.

- Configurar las directivas de red de anulación en los puertos

  Para aplicar diferentes directivas en los puertos distribuidos, se debe configurar la anulación por puerto de las directivas establecidas para el grupo de puertos. También se puede habilitar el restablecimiento de las opciones configuración que se establecen por puerto cuando un puerto distribuido se desconecta de una máquina virtual.

- Directiva de formación de equipos y conmutación por error

  La formación de equipos de NIC permite aumentar la capacidad de red de un conmutador virtual mediante la inclusión de dos o más NIC físicas en un equipo. Para determinar de qué forma se vuelve a enrutar el tráfico de red en caso de un error del adaptador, se deben incluir las NIC físicas en un orden de conmutación por error. Para determinar de qué forma el conmutador virtual distribuye el tráfico de red entre las NIC físicas en un equipo, se deben seleccionar los algoritmos de equilibrio de carga según las necesidades y capacidades del entorno.

- Directiva de VLAN

  Las directivas de VLAN determinan cómo funcionan las VLAN a través del entorno de red.

- Directiva de seguridad

  La directiva de seguridad de redes ayuda a proteger el tráfico contra la suplantación de direcciones MAC y la exploración de puertos no deseada.

- Directiva de catalogación de tráfico

  Una directiva de catalogación de tráfico se define por el ancho de banda promedio, el ancho de banda máximo y el tamaño de ráfaga. Se puede establecer una directiva de catalogación de tráfico para cada grupo de puertos y para cada puerto distribuido o grupo de puertos distribuidos.

- Directiva de asignación de recursos

  La directiva de asignación de recursos permite asociar un grupo de puertos o un puerto distribuido con un grupo de recursos de red creados por el usuario. Esta directiva proporciona mayor control sobre el ancho de banda asignado al puerto o al grupo de puertos.

- Directiva de supervisión

  La directiva de supervisión habilita o deshabilita la supervisión de NetFlow en un puerto o un grupo de puertos distribuidos.

- Directiva de filtrado y marcado de tráfico

  En vSphere Distributed Switch versión 5.5 y posteriores, la directiva de filtrado y marcado de tráfico permite proteger la red virtual ante el tráfico no deseado y los ataques de seguridad o aplicar una etiqueta de QoS a un tipo de tráfico específico.

- Administrar directivas para varios grupos de puertos en vSphere Distributed Switch

  Es posible modificar las directivas de redes para varios grupos de puertos en vSphere Distributed Switch.

- Directivas de bloqueo de puertos

  Las directivas de bloqueo de puertos permiten bloquear selectivamente el envío o la recepción de datos en los puertos.

Aplicar directivas de redes en vSphere Standard Switch o vSphere Distributed Switch

En vSphere Standard Switch y vSphere Distributed Switch se aplican directivas de redes diferentes. Algunas de las directivas disponibles para vSphere Distributed Switch no lo están para vSphere Standard Switch.

Tabla 8-1. Objetos del conmutador virtual donde se aplican las directivas

Conmutador virtual	Objeto del conmutador virtual	Descripción
vSphere Standard Switch	Conmutador completo	Cuando se aplican directivas en el conmutador estándar completo, las directivas se propagan a todos los grupos de puertos estándar del conmutador.
	Grupo de puertos estándar	Para aplicar diferentes directivas en los grupos de puertos individuales, se anulan las directivas heredadas del conmutador.

Tabla 8-1. Objetos del conmutador virtual donde se aplican las directivas (continuación)

Conmutador virtual	Objeto del conmutador virtual	Descripción
vSphere Distributed Switch	Grupo de puertos distribuidos	Cuando se aplican directivas en un grupo de puertos distribuidos, las directivas se propagan a todos los puertos del grupo.
	Puerto distribuido	Es posible aplicar diferentes directivas en los puertos distribuidos individuales. Para ello, se deben anular las directivas heredadas del grupo de puertos distribuidos.
	Grupo de puertos de vínculo superior	Se pueden aplicar directivas en el nivel del grupo de puertos de vínculo superior. Estas directivas se propagan a todos los puertos del grupo.
	Puerto de vínculo superior	Es posible aplicar diferentes directivas en los puertos individuales de vínculo superior. Para ello, se deben anular las directivas heredadas del grupo de puertos de vínculo superior.

Tabla 8-2. Directivas disponibles para vSphere Standard Switch y vSphere Distributed Switch

Directiva	Conmutador estándar	Distributed Switch	Descripción
Formación de equipos y conmutación por error	Sí	Sí	Permite configurar las NIC físicas que controlan el tráfico de red de un conmutador estándar, un grupo de puertos estándar, un grupo de puertos distribuidos y un puerto distribuido. Las NIC físicas se disponen en orden de conmutación por error, y a estas se les aplican diferentes directivas de equilibrio de carga.
Seguridad	Sí	Sí	Protege el tráfico contra la suplantación de direcciones MAC y la exploración de puertos no deseada. La directiva de seguridad de redes se implementa en la Capa 2 de la pila del protocolo de redes.
Catalogación de tráfico	Sí	Sí	Permite restringir el ancho de banda de red disponible en los puertos, pero también permite que ráfagas de tráfico circulen a velocidades mayores. ESXi cataloga el tráfico de red saliente en los conmutadores estándar y el tráfico entrante y saliente en los conmutadores distribuidos.
VLAN	Sí	Sí	Permite configurar el etiquetado de VLAN de un conmutador estándar o distribuido. Se pueden configurar el etiquetado de conmutador externo (EST), el etiquetado de conmutador virtual (VST) y el etiquetado de invitado virtual (VGT).
Supervisión	No	Sí	Habilita y deshabilita la supervisión de NetFlow en un puerto distribuido o un grupo de puertos.
Filtrado y marcado de tráfico	No	Sí	Permite proteger la red virtual frente al tráfico no deseado y a los ataques contra la seguridad, o bien aplicar una etiqueta de QoS a cierto tipo de tráfico.

Tabla 8-2. Directivas disponibles para vSphere Standard Switch y vSphere Distributed Switch (continuación)

Directiva	Conmutador estándar	Distributed Switch	Descripción
Asignación de recursos	No	Sí	Permite asociar un puerto distribuido o un grupo de puertos con un grupo de recursos de red definido por el usuario. De esta manera, se puede controlar mejor el ancho de banda disponible para el puerto o el grupo de puertos. La directiva de asignación de recursos se puede utilizar con vSphere Network I/O Control versión 2 y 3.
Bloqueo de puertos	No	Sí	Permite bloquear puertos selectivamente para el envío y la recepción de datos.

Configurar las directivas de red de anulación en los puertos

Para aplicar diferentes directivas en los puertos distribuidos, se debe configurar la anulación por puerto de las directivas establecidas para el grupo de puertos. También se puede habilitar el restablecimiento de las opciones configuración que se establecen por puerto cuando un puerto distribuido se desconecta de una máquina virtual.

Procedimiento

1 Busque un grupo de puertos distribuidos en vSphere Web Client.

   a Seleccione un conmutador distribuido y haga clic en la pestaña **Redes**.

   b Haga clic en **Grupos de puertos distribuidos**.

2 Haga clic con el botón derecho en el grupo de puertos distribuidos y seleccione **Editar configuración**.

3 Seleccione la página **Configuración avanzada**.

Opción	Descripción
Configurar el restablecimiento al desconectarse	En el menú desplegable, habilite o deshabilite el restablecimiento al desconectar. Cuando un puerto distribuido se desconecta de una máquina virtual, la configuración del puerto distribuido se restablece a la configuración del grupo de puertos distribuidos. Cualquier anulación por puerto se descartará.
Anular directivas de puerto	Seleccione las directivas del grupo de puertos distribuidos que se anularán por puerto.

4 (opcional) Use las páginas de directivas para establecer anulaciones para cada directiva de puerto.

5 Haga clic en **Aceptar**.

Directiva de formación de equipos y conmutación por error

La formación de equipos de NIC permite aumentar la capacidad de red de un conmutador virtual mediante la inclusión de dos o más NIC físicas en un equipo. Para determinar de qué forma se vuelve a enrutar el tráfico de red en caso de un error del adaptador, se deben incluir las NIC físicas en un orden de conmutación por error. Para determinar de qué forma el conmutador virtual distribuye el tráfico de red entre las NIC físicas en un equipo, se deben seleccionar los algoritmos de equilibrio de carga según las necesidades y capacidades del entorno.

Directiva de formación de equipos de NIC

Se puede utilizar la formación de equipos de NIC para conectar un conmutador virtual a varias NIC físicas en un host a fin de aumentar el ancho de banda de red del conmutador y proporcionar redundancia. Un equipo de NIC puede distribuir el tráfico entre sus miembros y proporcionar una conmutación por error pasiva en caso de que se produzca un error en el adaptador o una interrupción de la red. Las directivas de formación de equipos de NIC se establecen en el nivel del conmutador virtual o del grupo de puertos para vSphere Standard Switch, y en el nivel de puertos o de grupo de puertos para vSphere Distributed Switch.

Nota Todos los puertos del conmutador físico del mismo equipo deben encontrarse en el mismo dominio de difusión de Capa 2.

Directiva de equilibrio de carga

La directiva de equilibrio de carga determina de qué forma se distribuye el tráfico entre los adaptadores de red en un equipo de NIC. En los conmutadores virtuales de vSphere, el equilibrio de carga se aplica solamente al tráfico saliente. El tráfico entrante se controla con la directiva de equilibrio de carga en el conmutador físico.

Para obtener más información sobre cada algoritmo de equilibrio de carga, consulte Algoritmos de equilibrio de carga disponibles para los conmutadores virtuales.

Directiva de detección de errores de red

Se puede especificar uno de los siguientes métodos que el conmutador virtual puede utilizar para detectar la conmutación por error.

Solo estado de vínculo

Se basa solamente en el estado del vínculo que proporciona el adaptador de red. Detecta errores, como cables extraídos y fallas eléctricas en el conmutador físico. No obstante, el estado del vínculo no detecta los siguientes errores de configuración:

- Un puerto del conmutador físico bloqueado debido al árbol de expansión o una configuración errónea a la VLAN incorrecta.

- Un cable extraído que conecta el conmutador físico con otros dispositivos de redes, por ejemplo, un conmutador ascendente.

Sondeo de señal

Envía y escucha las tramas de difusión en Ethernet, o sondeos de señal, que las NIC físicas envían para detectar errores de vínculo en todas las NIC físicas de un equipo. Los hosts ESXi envían paquetes de señales cada segundo. El sondeo de señal resulta más útil para detectar errores en el conmutador físico más cercano al host ESXi, donde el error no provoca un evento de vínculo inactivo en el host.

El sondeo de señal se utiliza con tres o más NIC en un equipo debido a que ESXi puede detectar errores en un solo adaptador. Si se asignan solo dos NIC y una de ellas pierde conectividad, el conmutador no puede determinar qué NIC debe ponerse fuera de servicio porque ninguna de ellas recibe señales y, en consecuencia, todos los paquetes se envían a ambos vínculos superiores. La utilización de al menos tres NIC en un equipo permite que ocurran n-2 errores, donde *n* es la cantidad de NIC del equipo antes de que ocurra una situación ambigua.

Directiva de conmutación por recuperación

Una directiva de conmutación por recuperación se habilita de forma predeterminada en un equipo de NIC. Si una NIC física con errores vuelva a estar en línea, el conmutador virtual vuelve a poner la NIC en su estado activo reemplazando la NIC en espera que ocupó su ranura.

Si la NIC física que ocupa el primer lugar en el orden de conmutación por error tiene errores intermitentes, la directiva de conmutación por recuperación puede producir cambios frecuentes en la NIC utilizada. El conmutador físico advierte cambios frecuentes en las direcciones MAC; el puerto del conmutador físico podría no aceptar tráfico inmediatamente cuando un adaptador se pone en línea. Para minimizar estas demoras, se puede considerar cambiar la siguiente configuración del conmutador físico:

- Deshabilite el protocolo de árbol de expansión (Spanning Tree Protocol, STP) en las NIC físicas conectadas a los hosts ESXi.
- En las redes Cisco, habilite el modo PortFast para las interfaces de acceso o el modo PortFast troncal para las interfaces troncales. De este modo, se pueden ahorrar unos 30 segundos durante la inicialización del puerto del conmutador físico.
- Deshabilite la negociación de enlace troncal.

Directiva de notificación de conmutadores

Al utilizar la directiva de notificación de conmutadores, se puede determinar de qué forma el host ESXi comunica eventos de conmutación por error. Cuando una NIC física se conecta al conmutador virtual o cuando el tráfico se vuelve a enrutar a otra NIC física del equipo, el conmutador virtual envía notificaciones por medio de la red para actualizar las tablas de búsqueda en los conmutadores físicos. La notificación del conmutador físico ofrece la latencia más baja cuando se produce una conmutación por error o una migración con vSphere vMotion.

Algoritmos de equilibrio de carga disponibles para los conmutadores virtuales

Puede configurar diversos algoritmos de equilibrio de carga en un conmutador virtual para establecer cómo se distribuye el tráfico de red entre las NIC físicas de un equipo.

- Enrutar según el puerto virtual de origen

  El conmutador virtual selecciona vínculos superiores de acuerdo con los identificadores de puerto de la máquina virtual en vSphere Standard Switch o en vSphere Distributed Switch.

- Enrutar según el hash de MAC de origen

  El conmutador virtual selecciona un vínculo superior para una máquina virtual en función de la dirección MAC de la máquina virtual. Para calcular un vínculo superior para una máquina virtual, el conmutador virtual utiliza la dirección MAC de la máquina virtual y la cantidad de vínculos superiores del equipo de NIC.

- Enrutar según el hash de IP

  El conmutador virtual selecciona vínculos superiores para las máquinas virtuales de acuerdo con la dirección IP de origen y de destino de cada paquete.

- Enrutar según la carga de la NIC física

  El algoritmo Enrutar según la carga de la NIC física se basa en el algoritmo Enrutar según el puerto virtual de origen, por el cual el conmutador virtual comprueba la carga real de los vínculos superiores y sigue los pasos para reducirla en los vínculos superiores sobrecargados. Disponible solamente en vSphere Distributed Switch.

- Utilizar orden explícito de conmutación por error

  Con esta directiva no hay ningún equilibrio de carga disponible. El conmutador virtual usa siempre el vínculo superior que está en el primer lugar de la lista de adaptadores activos del orden de conmutación por error y que coincida con los criterios de detección para la conmutación por error. Si no hay vínculos superiores disponibles en la lista de adaptadores activos, el conmutador virtual usa los vínculos superiores de la lista de espera.

Enrutar según el puerto virtual de origen

El conmutador virtual selecciona vínculos superiores de acuerdo con los identificadores de puerto de la máquina virtual en vSphere Standard Switch o en vSphere Distributed Switch.

La ruta basada en el puerto virtual de origen es el método de equilibrio de carga predeterminado en un conmutador estándar de vSphere y en vSphere Distributed Switch.

Cada máquina virtual que se ejecuta en un host ESXi tiene un identificador de puerto virtual asociado en el conmutador virtual. Para calcular un vínculo superior para una máquina virtual, el conmutador virtual utiliza el identificador de puerto de la máquina virtual y la cantidad de vínculos superiores del equipo de NIC. Una vez que el conmutador virtual selecciona un vínculo superior

para una máquina virtual, siempre reenvía el tráfico a través del mismo vínculo superior para esta máquina virtual mientras la máquina se ejecute en el mismo puerto. El conmutador virtual calcula los vínculos superiores para las máquinas virtuales solamente una vez, excepto cuando se agregan vínculos superiores al equipo de NIC o se quitan de este equipo.

El identificador de puerto de una máquina virtual queda fijo mientras la máquina virtual se ejecuta en el mismo host. Si se migra, se apaga o se elimina la máquina virtual, el identificador de puerto en el conmutador virtual se libera. El conmutador virtual deja de enviar tráfico a través de este puerto, lo cual reduce el tráfico general del vínculo superior asociado. Si se apaga o se migra una máquina virtual, puede aparecer en otro puerto y utilizar el vínculo superior asociado con el nuevo puerto.

Tabla 8-3. Consideraciones sobre el uso de enrutar según el puerto virtual de origen

Consideraciones	Descripción
Ventajas	■ Una distribución equilibrada del tráfico si la cantidad de NIC virtuales es mayor que la cantidad de NIC físicas en el equipo. ■ Bajo consumo de recursos, ya que en la mayoría de los casos el conmutador virtual calcula los vínculos superiores para las máquinas virtuales una sola vez. ■ No se requieren cambios en el conmutador físico.
Desventajas	■ El conmutador virtual no reconoce la carga de tráfico de los vínculos superiores y no equilibra la carga del tráfico en los vínculos superiores con menos uso. ■ El ancho de banda disponible para una máquina virtual se limita a la velocidad del vínculo superior asociado con el identificador de puerto relevante, excepto que la máquina virtual tenga más de una NIC virtual.

Enrutar según el hash de MAC de origen

El conmutador virtual selecciona un vínculo superior para una máquina virtual en función de la dirección MAC de la máquina virtual. Para calcular un vínculo superior para una máquina virtual, el conmutador virtual utiliza la dirección MAC de la máquina virtual y la cantidad de vínculos superiores del equipo de NIC.

Tabla 8-4. Consideraciones sobre el uso de enrutar según el hash de MAC de origen

Consideraciones	Descripción
Ventajas	■ Se logra una distribución más equilibrada del tráfico que con la opción Enrutar según el puerto virtual de origen, ya que el conmutador virtual calcula un vínculo superior para cada paquete. ■ Las máquinas virtuales utilizan el mismo vínculo superior porque la dirección MAC es estática. Encender o apagar la máquina virtual no modifica el vínculo superior que utiliza la máquina virtual. ■ No se requieren cambios en el conmutador físico.
Desventajas	■ El ancho de banda disponible para la máquina virtual se limita a la velocidad del vínculo superior asociado con el identificador de puerto relevante, excepto que la máquina virtual utilice varias direcciones MAC de origen. ■ Más consumo de recursos que con la opción Enrutar según el puerto virtual de origen, ya que el conmutador virtual calcula un vínculo superior para cada paquete. ■ El conmutador virtual no reconoce la carga de los vínculos superiores, por lo que estos pueden sobrecargarse.

Enrutar según el hash de IP

El conmutador virtual selecciona vínculos superiores para las máquinas virtuales de acuerdo con la dirección IP de origen y de destino de cada paquete.

Para calcular un vínculo superior para una máquina virtual, el conmutador virtual toma el último octeto de las direcciones IP de origen y de destino del paquete, las procesa a través de una operación XOR y después procesa el resultado a través de otro cálculo en función de la cantidad de vínculos superiores en el equipo de NIC. El resultado es una cifra entre 0 y la cantidad de vínculos superiores del equipo menos uno. Por ejemplo, si un equipo de NIC tiene cuatro vínculos superiores, el resultado es una cifra entre 0 y 3, ya que cada número está asociado con una NIC del equipo. Para los paquetes que no utilizan IP, el conmutador virtual toma dos valores binarios de 32 bits de la trama o del paquete a fin de identificar la dirección IP.

Cualquier máquina virtual puede utilizar cualquier vínculo superior del equipo de NIC, según la dirección IP de origen y de destino. De esta forma, cada máquina virtual puede utilizar el ancho de banda de cualquier vínculo superior del equipo. Si una máquina virtual se ejecuta en un entorno donde hay una gran cantidad de máquinas virtuales independientes, el algoritmo de hash de IP permite una división uniforme del tráfico entre las NIC del equipo. Cuando una máquina virtual se comunica con varias direcciones IP de destino, el conmutador virtual puede generar un hash diferente para cada IP de destino. De esta forma, los paquetes pueden utilizar vínculos superiores diferentes en el conmutador virtual y así lograr una mejor capacidad de proceso potencial.

Sin embargo, si el entorno tiene una cantidad reducida de direcciones IP, es posible que el conmutador virtual haga pasar constantemente el tráfico por un mismo vínculo superior del equipo. Por ejemplo, si tiene un servidor de base de datos al que accede un servidor de aplicaciones, el conmutador virtual siempre calcula el mismo vínculo superior, ya que solo hay un par de origen y destino.

Configuración del conmutador físico

Para asegurarse de que el equilibrio de carga según el hash de IP funcione correctamente, debe haber un EtherChannel configurado en el conmutador físico. Un EtherChannel enlaza varios adaptadores de red en un mismo vínculo lógico. Cuando los puertos se enlazan a un EtherChannel, cada vez que el conmutador físico recibe un paquete de la misma dirección MAC de máquina virtual, el conmutador actualiza correctamente la tabla de memoria de direcciones de contenido (CAM).

Por ejemplo, si el conmutador físico recibe paquetes en los puertos 01 y 02 desde la dirección MAC A, el conmutador agrega una entrada 01-A y 02-A en su tabla de CAM. En consecuencia, el conmutador físico distribuye el tráfico entrante a los puertos correctos. Si no tiene un EtherChannel, el conmutador físico indica en el registro que se recibió un paquete desde la dirección MAC A en el puerto 01, después actualiza el mismo registro para indicar que se recibió un paquete de la dirección MAC A en el puerto 02. Por lo tanto, el conmutador físico reenvía el tráfico entrante únicamente a través del puerto 02, por lo que algunos paquetes no llegarían a su destino y se sobrecargaría el vínculo superior correspondiente.

Limitaciones y requisitos de configuración

- Los hosts ESXi admiten la formación de equipos de hash de IP en un mismo conmutador físico o en conmutadores apilados.
- Los hosts ESXi solamente admiten la adición de enlaces 802.3ad en el modo estático. Puede utilizar un solo EtherChannel estático con vSphere Standard Switch. No se admite LACP. Para utilizar LACP debe contar con vSphere Distributed Switch 5.1, o una versión posterior, o Cisco Nexus 1000V. Si habilita el equilibrio de carga según el hash de IP sin adición de enlaces 802.3ad, y viceversa, pueden producirse interrupciones de redes.
- Debe utilizar la opción Solo estado de vínculo para la detección errores de red cuando se usa el equilibrio de carga según el hash de IP.
- Debe configurar todos los vínculos superiores del equipo en la lista de conmutación por error activa. Las listas de elementos en espera y sin uso deben estar vacías.
- La cantidad de puertos del EtherChannel debe ser igual a la cantidad de vínculos superiores del equipo.

Consideraciones sobre el uso del enrutamiento según el hash de IP

Consideraciones	Descripción
Ventajas	■ Se logra una distribución más uniforme de la carga que con las opciones Enrutar según el puerto virtual de origen y Enrutar según el hash de MAC de origen, ya que el conmutador calcula el vínculo superior de cada paquete. ■ Una mejor capacidad de proceso potencial para las máquinas virtuales que se comunican con varias direcciones IP.
Desventajas	■ Más consumo de recursos que con los demás algoritmos de equilibrio de carga. ■ El conmutador virtual no reconoce la carga real de los vínculos superiores. ■ Se requieren cambios en la red física. ■ El proceso de solución de problemas es complejo.

Enrutar según la carga de la NIC física

El algoritmo Enrutar según la carga de la NIC física se basa en el algoritmo Enrutar según el puerto virtual de origen, por el cual el conmutador virtual comprueba la carga real de los vínculos superiores y sigue los pasos para reducirla en los vínculos superiores sobrecargados. Disponible solamente en vSphere Distributed Switch.

El conmutador distribuido calcula los vínculos superiores de las máquinas virtuales sobre la base de su identificador de puerto y la cantidad de vínculos superiores en el equipo de la NIC. El conmutador distribuido prueba los vínculos superiores cada 30 segundos. Si la carga supera el 75 % de la utilización, el identificador de puerto de la máquina virtual con la E/S más alta se transfiere a otro vínculo superior.

Tabla 8-5. Consideraciones sobre el uso de Enrutar según la carga de la NIC física

Consideraciones	Descripción
Ventajas	■ El consumo de recursos es bajo, ya que el conmutador distribuido calcula los vínculos superiores de las máquinas virtuales una sola vez y la comprobación de los vínculos superiores produce un impacto mínimo. ■ El conmutador distribuido reconoce la carga de los vínculos superiores y se ocupa de reducirla si es necesario. ■ No se requieren cambios en el conmutador físico.
Desventajas	■ El ancho de banda disponible en las máquinas virtuales se limita a los vínculos superiores que están conectados al conmutador distribuido.

Utilizar orden explícito de conmutación por error

Con esta directiva no hay ningún equilibrio de carga disponible. El conmutador virtual usa siempre el vínculo superior que está en el primer lugar de la lista de adaptadores activos del orden de conmutación por error y que coincida con los criterios de detección para la conmutación por error. Si no hay vínculos superiores disponibles en la lista de adaptadores activos, el conmutador virtual usa los vínculos superiores de la lista de espera.

Configurar la formación de equipos de NIC, la conmutación por error y el equilibrio de carga en vSphere Standard Switch o un grupo de puertos estándar

Incluya dos o más NIC físicas en un equipo para aumentar la capacidad de la red de vSphere Standard Switch o un grupo de puertos estándar. Configure el orden de conmutación por error para establecer de qué forma se vuelve a enrutar el tráfico de red en caso de un error del adaptador. Seleccione un algoritmo de equilibrio de carga para determinar cómo distribuye el conmutador estándar el tráfico entre las NIC físicas de un equipo.

Configure la formación de equipos de NIC, la conmutación por error y el equilibrio de carga de acuerdo con la configuración de la red en el conmutador físico y la topología del conmutador estándar. Para obtener más información, consulte Directiva de formación de equipos y conmutación por error y Algoritmos de equilibrio de carga disponibles para los conmutadores virtuales.

Si configura la directiva de formación de equipos y conmutación por error en un conmutador estándar, la directiva se propaga a todos los grupos de puertos del conmutador. Si se configura la directiva en un grupo de puertos estándar, se anula la directiva heredada del conmutador.

Procedimiento

1. En vSphere Web Client, desplácese hasta el host.
2. En la pestaña **Configurar**, expanda **Redes** y seleccione **Conmutadores virtuales**.
3. Desplácese hasta la directiva de formación de equipos y conmutación por error del conmutador estándar o del grupo de puertos estándar.

Opción	Acción
Conmutador estándar	a Seleccione el conmutador en la lista. b Haga clic en **Editar configuración** y seleccione **Formación de equipos y conmutación por error**.
Grupo de puertos estándar	a Seleccione el conmutador donde reside el grupo de puertos. b En el diagrama de topología del conmutador, seleccione el grupo de puertos estándar y haga clic en **Editar configuración**. c Seleccione **Formación de equipos y conmutación por error**. d Seleccione **Anular** junto a las directivas que desea anular.

4 En el menú desplegable **Equilibrio de carga**, especifique cómo la carga del conmutador virtual equilibra el tráfico saliente entre las NIC físicas de un equipo.

Opción	Descripción
Enrutar según el puerto virtual de origen	Seleccione un vínculo superior en función de los identificadores de los puertos virtuales del conmutador. Una vez que el conmutador virtual selecciona un vínculo superior para una máquina virtual o un adaptador VMkernel, envía el tráfico siempre por el mismo vínculo superior para esa máquina virtual o ese adaptador VMkernel.
Enrutar según el hash de IP	Seleccione un vínculo superior según el hash de las direcciones IP de origen y destino de cada paquete. En los paquetes que no utilizan IP, el conmutador utiliza los datos de esos campos para calcular el hash. La formación de equipos basada en IP requiere que el conmutador físico se configure en EtherChannel.
Enrutar según el hash de MAC de origen	Seleccione un vínculo superior según un hash de la Ethernet de origen.
Utilizar orden explícito de conmutación por error	En la lista de adaptadores activos, utilice siempre el vínculo superior de orden más alto que pasa los criterios de detección de conmutación por error. No se realiza ningún equilibrio de carga mediante esta opción.

5 En el menú desplegable **Detección de errores de red**, seleccione el método que utiliza el conmutador virtual para la detección de conmutación por error.

Opción	Descripción
Solo estado de vínculo	Se basa solamente en el estado del vínculo que proporciona el adaptador de red. Esta opción detecta errores como cables extraídos o fallas eléctricas en el conmutador físico.
Sondeo de señal	Envía y escucha las sondas de señal en todas las NIC del equipo y utiliza esta información, junto con el estado del vínculo, para determinar el error en el vínculo. ESXi envía paquetes de señales a cada segundo. Las NIC deben estar configuradas como activa/activa o activa/en espera debido a que las NIC con un estado sin utilizar no participan en el sondeo de señal.

6 En el menú desplegable **Notificar a conmutadores**, seleccione si el conmutador distribuido o estándar notifica al conmutador físico en caso de una conmutación por error.

Nota Establezca esta opción en **No** si una máquina virtual conectada está utilizando el equilibrio de carga de red de Microsoft en el modo de unidifusión. No existen problemas si el equilibrio de carga de red se ejecuta en modo de multidifusión.

7 En el menú desplegable **Conmutación por recuperación**, seleccione si un adaptador físico volverá al estado activo después de recuperarse de un error.

Si la conmutación por recuperación se establece en **Sí**, que es la selección predeterminada, el adaptador vuelve al servicio activo inmediatamente después de la recuperación, desplazando a cualquier adaptador en espera que hubiera ocupado su ranura.

Si la conmutación por recuperación se establece en **No** para un puerto estándar, el adaptador con errores se deja inactivo después de la recuperación hasta que otro adaptador actualmente activo presente error y requiera su sustitución.

8 Configure la lista Orden de conmutación por error para especificar cómo se utilizan los vínculos superiores en un equipo cuando se produce una conmutación por error.

Si desea utilizar algunos vínculos superiores y reservar otros para utilizarlos en caso de que los vínculos en uso presenten errores, utilice las flechas hacia arriba y hacia abajo para mover los vínculos superiores a diferentes grupos.

Opción	Descripción
Adaptadores activos	Siga utilizando el vínculo superior si la conectividad del adaptador de red está activa y en funcionamiento.
Adaptadores en espera	Utilice este vínculo superior si uno de los adaptadores físicos activos está desactivado.
Adaptadores sin utilizar	No utilice este vínculo superior.

9 Haga clic en **Aceptar**.

Configurar formación de equipos de NIC, conmutación por error y equilibrio de carga en un grupo de puertos distribuidos o un puerto distribuido

Incluya dos o más NIC físicas en un equipo para aumentar la capacidad de red de un puerto o un grupo de puertos distribuidos. Configure el orden de conmutación por error para establecer de qué forma se vuelve a enrutar el tráfico de red en caso de un error del adaptador. Seleccione un algoritmo de equilibrio de carga para determinar de qué forma el conmutador distribuido aplica el equilibrio de carga al tráfico entre las NIC físicas de un equipo.

Configure la formación de equipos de NIC, la conmutación por error y el equilibrio de carga de acuerdo con la configuración de la red en el conmutador físico y la topología del conmutador distribuido. Para obtener más información, consulte Directiva de formación de equipos y conmutación por error y Algoritmos de equilibrio de carga disponibles para los conmutadores virtuales.

Si configura la directiva de formación de equipos y conmutación por error para un grupo de puertos distribuidos, la directiva se propaga a todos los puertos del grupo. Si se configura la directiva para un puerto distribuido, se anula la directiva heredada del grupo.

Requisitos previos

Para anular una directiva en el nivel del puerto distribuido, habilite la opción de anulación en el nivel de puerto para esta directiva. Consulte Configurar las directivas de red de anulación en los puertos.

Procedimiento

1 En vSphere Web Client, desplácese hasta el conmutador distribuido.

2 Desplácese hasta la directiva de formación de equipos y conmutación por error del puerto o del grupo de puertos distribuidos.

Opción	Acción
Grupo de puertos distribuidos	a En el menú **Acciones** seleccione **Grupo de puertos distribuidos > Administrar grupos de puertos distribuidos**. b Seleccione **Formación de equipos y conmutación por error**. c Seleccione el grupo de puertos y haga clic en **Siguiente**.
Puerto distribuido	a En la pestaña **Redes**, haga clic en **Grupos de puertos distribuidos** y, a continuación, haga doble clic en un grupo de puertos distribuidos. b En la pestaña **Puertos**, seleccione un puerto y haga clic en **Editar configuración de puertos distribuidos**. c Seleccione **Formación de equipos y conmutación por error**. d Seleccione **Anular** junto a las propiedades que desea anular.

3 En el menú desplegable **Equilibrio de carga**, especifique cómo la carga del conmutador virtual equilibra el tráfico saliente entre las NIC físicas de un equipo.

Opción	Descripción
Enrutar según el puerto virtual de origen	Seleccione un vínculo superior en función de los identificadores de los puertos virtuales del conmutador. Una vez que el conmutador virtual selecciona un vínculo superior para una máquina virtual o un adaptador VMkernel, envía el tráfico siempre por el mismo vínculo superior para esa máquina virtual o ese adaptador VMkernel.
Enrutar según el hash de IP	Seleccione un vínculo superior según el hash de las direcciones IP de origen y destino de cada paquete. En los paquetes que no utilizan IP, el conmutador utiliza los datos de esos campos para calcular el hash. La formación de equipos basada en IP requiere que el conmutador físico se configure en EtherChannel.
Enrutar según el hash de MAC de origen	Seleccione un vínculo superior según un hash de la Ethernet de origen.
Enrutar según la carga de la NIC física	Disponible para puertos distribuidos o grupos de puertos distribuidos. Seleccione un vínculo superior basado en la carga actual de los adaptadores de red físicos conectados al puerto o al grupo de puertos. Si un vínculo superior permanece ocupado al 75 % o más durante 30 segundos, el conmutador proxy del host mueve una parte del tráfico de la máquina virtual a un adaptador físico con capacidad libre.
Utilizar orden explícito de conmutación por error	En la lista de adaptadores activos, utilice siempre el vínculo superior de orden más alto que pasa los criterios de detección de conmutación por error. No se realiza ningún equilibrio de carga mediante esta opción.

4 En el menú desplegable **Detección de errores de red**, seleccione el método que utiliza el conmutador virtual para la detección de conmutación por error.

Opción	Descripción
Solo estado de vínculo	Se basa solamente en el estado del vínculo que proporciona el adaptador de red. Esta opción detecta errores como cables extraídos o fallas eléctricas en el conmutador físico.
Sondeo de señal	Envía y escucha las sondas de señal en todas las NIC del equipo y utiliza esta información, junto con el estado del vínculo, para determinar el error en el vínculo. ESXi envía paquetes de señales a cada segundo. Las NIC deben estar configuradas como activa/activa o activa/en espera debido a que las NIC con un estado sin utilizar no participan en el sondeo de señal.

5 En el menú desplegable **Notificar a conmutadores**, seleccione si el conmutador distribuido o estándar notifica al conmutador físico en caso de una conmutación por error.

Nota Establezca esta opción en **No** si una máquina virtual conectada está utilizando el equilibrio de carga de red de Microsoft en el modo de unidifusión. No existen problemas si el equilibrio de carga de red se ejecuta en modo de multidifusión.

6 En el menú desplegable **Conmutación por recuperación**, seleccione si un adaptador físico volverá al estado activo después de recuperarse de un error.

Si la conmutación por recuperación se establece en **Sí**, que es la selección predeterminada, el adaptador vuelve al servicio activo inmediatamente después de la recuperación, desplazando a cualquier adaptador en espera que hubiera ocupado su ranura.

Si la conmutación por recuperación se establece en **No** para un puerto distribuido, el adaptador con errores se deja inactivo después de la recuperación solo si la máquina virtual asociada está en ejecución. Cuando la opción **Conmutación por recuperación** es **No** y la máquina virtual está apagada, si todos los adaptadores físicos presentan errores y, a continuación, uno de ellos se recupera, la NIC virtual se conecta al adaptador recuperado en lugar de hacerlo a uno en espera una vez que se enciende la máquina virtual. Si se apaga y se enciende la máquina virtual, la NIC virtual se vuelva a conectar al puerto distribuido. El conmutador distribuido considera el puerto como recién agregado y le asigna el puerto de vínculo superior predeterminado, es decir, el adaptador de vínculo superior activo.

7 Configure la lista Orden de conmutación por error para especificar cómo se utilizan los vínculos superiores en un equipo cuando se produce una conmutación por error.

Si desea utilizar algunos vínculos superiores y reservar otros para utilizarlos en caso de que los vínculos en uso presenten errores, utilice las flechas hacia arriba y hacia abajo para mover los vínculos superiores a diferentes grupos.

Opción	Descripción
Adaptadores activos	Siga utilizando el vínculo superior si la conectividad del adaptador de red está activa y en funcionamiento.
Adaptadores en espera	Utilice este vínculo superior si uno de los adaptadores físicos activos está desactivado.
Adaptadores sin utilizar	No utilice este vínculo superior.

8 Revise las opciones y aplique la configuración.

Directiva de VLAN

Las directivas de VLAN determinan cómo funcionan las VLAN a través del entorno de red.

Una red de área local virtual (VLAN) es un grupo de hosts con un conjunto común de requisitos, que se comunican como si estuvieran asociados a un mismo dominio de difusión, independientemente de su ubicación física. Una VLAN tiene los mismos atributos que una red de área local (LAN) física, pero permite que las estaciones finales se agrupen aunque no estén en el mismo conmutador de red.

El alcance de las directivas de VLAN pueden ser puertos y grupos de puertos distribuidos, y puertos y grupos de puertos de vínculo superior.

Configurar etiquetado de VLAN en un grupo de puertos distribuidos o un puerto distribuido

Para aplicar globalmente el etiquetado de VLAN en todos los puertos distribuidos, es necesario configurar la directiva de VLAN en un grupo de puertos distribuidos. Para integrar el tráfico virtual en el puerto con VLAN físicas con un método diferente al del grupo de puertos distribuidos primario, se debe usar la directiva de VLAN en un puerto distribuido.

Requisitos previos

Para anular una directiva en el nivel del puerto distribuido, habilite la opción de anulación en el nivel de puerto para esta directiva. Consulte Configurar las directivas de red de anulación en los puertos.

Procedimiento

1 En vSphere Web Client, desplácese hasta el conmutador distribuido.

2 Desplácese hasta la directiva de VLAN en el grupo de puertos distribuidos o en el puerto distribuido.

Opción	Acción
Grupo de puertos distribuidos	a En el menú **Acciones** seleccione **Grupo de puertos distribuidos > Administrar grupos de puertos distribuidos**. b Seleccione **VLAN** y haga clic en **Siguiente**. c Seleccione el grupo de puertos y haga clic en **Siguiente**.
Puerto distribuido	a En la pestaña **Redes**, haga clic en **Grupos de puertos distribuidos** y, a continuación, haga doble clic en un grupo de puertos distribuidos. b En la pestaña **Puertos**, seleccione un puerto y haga clic en el icono **Editar configuración de puertos distribuidos**. c Seleccione **VLAN**. d Seleccione **Anular** junto a las propiedades que desea anular.

3 En el menú desplegable **Tipo de VLAN**, seleccione el tipo de filtrado y marcado del tráfico de VLAN y haga clic en **Siguiente**.

Opción	Descripción
Ninguna	No utilice la VLAN. Utilice esta opción en caso de etiquetado de conmutador externo.
VLAN	Etiquete el tráfico con el identificador del campo **Identificador de VLAN**. Escriba un número entre 1 y 4094 para el etiquetado de conmutador virtual.
Enlace troncal de VLAN	Pase el tráfico de VLAN con identificador dentro de **Rango troncales de VLAN** al sistema operativo invitado. Se pueden configurar varios rangos y VLAN individuales utilizando una lista separada por comas. Por ejemplo: `1702-1705, 1848-1849`. Utilice esta opción para el etiquetado de invitado virtual.
VLAN privada	Asocie el tráfico con una VLAN privada creada en el conmutador distribuido.

4 Revise las opciones y aplique la configuración.

Configurar del etiquetado de VLAN en un grupo de puertos de vínculo superior o un puerto de vínculo superior

Para configurar el procesamiento de tráfico de VLAN general para todos los vínculos superiores que son miembros, se debe configurar la directiva de VLAN en un puerto de vínculo superior. Para controlar el tráfico de VLAN a través del puerto de una forma diferente a la del grupo de puertos de vínculo superior primario, se debe establecer la directiva de VLAN en un vínculo superior.

Utilice la directiva de VLAN en el nivel del puerto de vínculo superior para propagar un rango troncal de varios identificadores de VLAN a los adaptadores de red físicos para el filtrado de tráfico. Los adaptadores de red físicos descartan los paquetes de las otras VLAN si los adaptadores admiten el filtrado de VLAN. La configuración de un rango troncal mejora el rendimiento de las redes porque los adaptadores de red físicos filtran el tráfico en lugar de los puertos de vínculo superior en el grupo.

Si tiene un adaptador de red físico que no admita el filtrado de VLAN, es posible que las VLAN no estén bloqueadas. En este caso, configure el filtrado de VLAN en un grupo de puertos distribuidos o en un puerto distribuido.

Para obtener información sobre la compatibilidad con el filtrado de VLAN, consulte la documentación técnica de los proveedores de los adaptadores.

Requisitos previos

Para anular la directiva de VLAN en el nivel de puerto, habilite las anulaciones en el nivel de puerto. Consulte Configurar las directivas de red de anulación en los puertos.

Procedimiento

1 En vSphere Web Client, desplácese hasta un conmutador distribuido.

2 En la pestaña **Redes**, haga clic en **Grupos de puertos de vínculo superior**.

3 Desplácese hasta la directiva de VLAN en el puerto o el grupo de puertos de vínculo superior.

Opción	Acción
Grupo de puertos de vínculo superior	a Haga clic con el botón derecho en un grupo de puertos de vínculo superior en la lista y seleccione **Editar configuración**. b Haga clic en **VLAN**.
Puerto de vínculo superior	a Haga doble clic en un grupo de puertos de vínculo superior. b En la pestaña **Puertos**, seleccione un puerto y haga clic en la pestaña **Editar configuración de puertos distribuidos**. c Haga clic en **VLAN** y seleccione **Anular**.

4 Escriba un valor para **Rango troncales de VLAN** para propagarlo a los adaptadores de red físicos.

Para realizar el enlace troncal de varios rangos y VLAN individuales, separe las entradas con comas.

5 Haga clic en **Aceptar**.

Directiva de seguridad

La directiva de seguridad de redes ayuda a proteger el tráfico contra la suplantación de direcciones MAC y la exploración de puertos no deseada.

La directiva de seguridad de un conmutador estándar o distribuido se implementa en la Capa 2 (capa de vínculo de datos) de la pila del protocolo de red. Los tres elementos de la directiva de seguridad son el modo promiscuo, los cambios de dirección MAC y las transmisiones falsificadas. Consulte la documentación de *Seguridad de vSphere* para obtener información sobre posibles amenazas para las redes.

Configurar la directiva de seguridad de vSphere Standard Switch o un grupo de puertos estándar

En vSphere Standard Switch, puede configurar para que la directiva de seguridad rechace los cambios de dirección MAC y de modo promiscuo en el sistema operativo invitado de una máquina virtual. Puede anular la directiva de seguridad que se hereda del conmutador estándar en grupos de puertos individuales.

Procedimiento

1. En vSphere Web Client, desplácese hasta el host.
2. En la pestaña **Configurar**, expanda **Redes** y seleccione **Conmutadores virtuales**.
3. Desplácese hasta la directiva de seguridad del conmutador o del grupo de puertos estándar.

Opción	Acción
Conmutador estándar de vSphere	a Seleccione de la lista un conmutador estándar. b Haga clic en **Editar configuración**. c Seleccione **Seguridad**.
Grupo de puertos estándar	a Seleccione el conmutador estándar donde reside el grupo de puertos. b En el diagrama de topología, seleccione un grupo de puertos estándar. c Haga clic en **Editar configuración**. d Seleccione **Seguridad** y, a continuación, **Anular** junto a las opciones que desee anular.

4 Rechace o acepte la activación del modo promiscuo o los cambios de dirección MAC en el sistema operativo invitado de las máquinas virtuales asociadas al conmutador o al grupo de puertos estándar.

Opción	Descripción
Modo promiscuo	■ **Rechazar**. El adaptador de red de máquina virtual recibe únicamente tramas dirigidas a la máquina virtual. ■ **Aceptar**. El conmutador virtual envía todas las tramas a la máquina virtual de acuerdo con la directiva de VLAN vigente para el puerto en el cual está conectado el adaptador de red de máquina virtual. **Nota** El modo promiscuo no es un modo seguro de funcionamiento. Los firewall, los escáneres de puertos y los sistemas de detección de intrusiones deben ejecutarse en modo promiscuo.
Cambios de dirección MAC	■ **Rechazar**. Si el sistema operativo invitado cambia la dirección MAC efectiva de la máquina virtual a un valor diferente de la dirección MAC del adaptador de red de máquina virtual (establecido en el archivo de configuración de `.vmx`), el conmutador descarta todas las tramas entrantes al adaptador. Si el sistema operativo invitado vuelve a cambiar la dirección MAC efectiva de la máquina virtual a la dirección MAC del adaptador de red de máquina virtual, la máquina virtual recibe las tramas nuevamente. ■ **Aceptar**. Si el sistema operativo invitado cambia la dirección MAC efectiva de la máquina virtual a un valor distinto de la dirección MAC del adaptador de red de máquina virtual, el conmutador permite que pasen las tramas a la dirección nueva.
Transmisiones falsificadas	■ **Rechazar**. el conmutador descarta cualquier trama saliente desde el adaptador de máquina virtual con una dirección MAC de origen que sea diferente de la que aparece en el archivo de configuración `.vmx`. ■ **Aceptar**. El conmutador no filtra y acepta todas las tramas salientes.

5 Haga clic en **Aceptar**.

Configurar la directiva de seguridad para un puerto distribuido o un grupo de puertos distribuidos

Establezca una directiva de seguridad en un grupo de puertos distribuidos para permitir o rechazar el modo promiscuo y los cambios de dirección MAC desde el sistema operativo invitado de las máquinas virtuales asociadas con el grupo de puertos. Se puede anular la directiva de seguridad heredada de los grupos de puertos distribuidos en puertos individuales.

Requisitos previos

Para anular una directiva en el nivel del puerto distribuido, habilite la opción de anulación en el nivel de puerto para esta directiva. Consulte Configurar las directivas de red de anulación en los puertos.

Procedimiento

1 En vSphere Web Client, desplácese hasta el conmutador distribuido.

2 Desplácese hasta la directiva de seguridad para el grupo de puertos distribuidos o el puerto distribuido.

Opción	Acción
Grupo de puertos distribuidos	a En el menú **Acciones** seleccione **Grupo de puertos distribuidos > Administrar grupos de puertos distribuidos**. b Seleccione **Seguridad**. c Seleccione el grupo de puertos y haga clic en **Siguiente**.
Puerto distribuido	a En la pestaña **Redes**, haga clic en **Grupos de puertos distribuidos** y, a continuación, haga doble clic en un grupo de puertos distribuidos. b En la pestaña **Puertos**, seleccione un puerto y haga clic en el icono **Editar configuración de puertos distribuidos**. c Seleccione **Seguridad**. d Seleccione **Anular** junto a las propiedades que desea anular.

3 Rechace o acepte la activación del modo promiscuo o los cambios de dirección MAC en el sistema operativo invitado de las máquinas virtuales asociadas al puerto distribuido o al grupo de puertos distribuidos.

Opción	Descripción
Modo promiscuo	■ **Rechazar**. El adaptador de red de máquina virtual recibe únicamente tramas dirigidas a la máquina virtual. ■ **Aceptar**. El conmutador virtual envía todas las tramas a la máquina virtual de acuerdo con la directiva de VLAN vigente para el puerto en el cual está conectado el adaptador de red de máquina virtual. **Nota** El modo promiscuo no es un modo seguro de funcionamiento. Los firewall, los escáneres de puertos y los sistemas de detección de intrusiones deben ejecutarse en modo promiscuo.
Cambios de dirección MAC	■ **Rechazar**. Si el sistema operativo invitado cambia la dirección MAC efectiva de la máquina virtual a un valor diferente de la dirección MAC del adaptador de red de máquina virtual (establecido en el archivo de configuración de `.vmx`), el conmutador descarta todas las tramas entrantes al adaptador. Si el sistema operativo invitado vuelve a cambiar la dirección MAC efectiva de la máquina virtual a la dirección MAC del adaptador de red de máquina virtual, la máquina virtual recibe las tramas nuevamente. ■ **Aceptar**. Si el sistema operativo invitado cambia la dirección MAC efectiva de la máquina virtual a un valor distinto de la dirección MAC del adaptador de red de máquina virtual, el conmutador permite que pasen las tramas a la dirección nueva.
Transmisiones falsificadas	■ **Rechazar**. el conmutador descarta cualquier trama saliente desde el adaptador de máquina virtual con una dirección MAC de origen que sea diferente de la que aparece en el archivo de configuración `.vmx`. ■ **Aceptar**. El conmutador no filtra y acepta todas las tramas salientes.

4 Revise las opciones y aplique la configuración.

Directiva de catalogación de tráfico

Una directiva de catalogación de tráfico se define por el ancho de banda promedio, el ancho de banda máximo y el tamaño de ráfaga. Se puede establecer una directiva de catalogación de tráfico para cada grupo de puertos y para cada puerto distribuido o grupo de puertos distribuidos.

ESXi cataloga el tráfico de red saliente en los conmutadores estándar y el tráfico entrante y saliente en los conmutadores distribuidos. La catalogación de tráfico restringe el ancho de banda de red disponible en un puerto, pero también se puede configurar para permitir que las ráfagas de tráfico atraviesen a velocidades más altas.

Ancho de banda promedio

Establece la cantidad de bits por segundo permitida para atravesar un puerto, promediada en el tiempo. Esta cantidad es la carga promedio permitida.

Ancho de banda máximo

La cantidad máxima de bits por segundo permitida para atravesar un puerto cuando este envía o recibe una ráfaga de tráfico. Esta cantidad limita el ancho de banda que utiliza un puerto cuando está utilizando su ráfaga adicional.

Tamaño de ráfaga

La cantidad máxima de bytes que se permite en una ráfaga. Si se establece este parámetro, un puerto podría obtener una ráfaga adicional si no utiliza todo su ancho de banda asignado. Cuando el puerto necesita más ancho de banda que el especificado por el ancho de banda promedio, se le puede permitir la transmisión temporal de datos a una velocidad superior si hay una ráfaga adicional disponible. Este parámetro limita la cantidad de bytes que se acumularon en la ráfaga adicional y transfiere el tráfico a una velocidad mayor.

Configurar la catalogación de tráfico de vSphere Standard Switch o grupo de puertos estándar

ESXi permite catalogar el tráfico saliente en los conmutadores o los grupos de puertos estándar. El catalogador de tráfico restringe el ancho de banda de red disponible para cualquier puerto, pero también es posible configurarlo para permitir temporalmente ráfagas de tráfico que pasen a través de un puerto a velocidades mayores.

Las directivas de catalogación de tráfico que se establecen para un conmutador o un grupo de puertos se aplican a cada puerto individual que forma parte del conmutador o grupo de puertos. Por ejemplo, si establece un ancho de banda promedio de 100.000 Kbps en un grupo de puertos estándar, un promedio de 100.000 Kbps puede pasar por cada puerto asociado al grupo de puertos estándar.

Procedimiento

1 En vSphere Web Client, desplácese hasta el host.

2 En la pestaña **Configurar**, expanda **Redes** y seleccione **Conmutadores virtuales**.

3 Desplácese hasta la directiva de catalogación de tráfico en el conmutador o grupo de puertos estándar.

Opción	Acción
vSphere Standard Switch	a Seleccione de la lista un conmutador estándar. b Haga clic en **Editar configuración**. c Seleccione **Catalogación de tráfico**.
Grupo de puertos estándar	a Seleccione el conmutador estándar donde reside el grupo de puertos. b En el diagrama de topología, seleccione un grupo de puertos estándar. c Haga clic en **Editar configuración**. d Seleccione **Catalogación de tráfico** y, a continuación, **Anular** junto a las opciones que desee anular.

4 Configure las directivas de catalogación de tráfico.

Opción	Descripción
Estado	Habilita los límites de configuración para la cantidad de ancho de banda de redes asignado a cada puerto asociado con el conmutador o el grupo de puertos estándar.
Ancho de banda promedio	Establece la cantidad de bits por segundo que se permitirá en un puerto, con un promedio a lo largo del tiempo (carga promedio permitida).
Ancho de banda máximo	La cantidad máxima de bits por segundo que se permite en un puerto para el envío de una ráfaga de tráfico. Esta configuración supera el ancho de banda utilizado por un puerto cuando aplica su ráfaga adicional. Este parámetro nunca puede ser inferior al ancho de banda promedio.
Tamaño de ráfaga	Es la cantidad máxima de bytes que se permiten en una ráfaga. Si se establece este parámetro, un puerto podría recibir una ráfaga adicional cuando no utiliza todo el ancho de banda asignado. Si el puerto necesita más ancho de banda que el promedio especificado, el puerto puede transmitir datos temporalmente a una velocidad superior si hay una ráfaga adicional disponible. Este parámetro aumenta la cantidad de bytes que se pueden acumular en la ráfaga adicional y transferir a una velocidad mayor.

5 Para cada directiva de catalogación de tráfico (**Ancho de banda promedio**, **Ancho de banda pico** y **Tamaño de ráfaga**), introduzca un valor de ancho de banda.

6 Haga clic en **Aceptar**.

Editar la directiva de catalogación de tráfico en un grupo de puertos distribuidos o un puerto distribuido

Puede catalogar el tráfico entrante o saliente de los grupos de puertos distribuidos o los puertos distribuidos de vSphere. El catalogador de tráfico restringe el ancho de banda de red para cualquier puerto del grupo, pero también es posible configurarlo para permitir temporalmente que “ráfagas” de tráfico pasen a través de un puerto a velocidades mayores.

Las directivas de catalogación de tráfico que se establecen para un grupo de puertos distribuidos se aplican a cada puerto individual que forma parte del grupo de puertos. Por ejemplo, si establece un ancho de banda promedio de 100.000 Kbps en un grupo de puertos distribuidos, un promedio de 100.000 Kbps puede pasar por cada puerto asociado al grupo de puertos distribuidos.

Requisitos previos

Para anular una directiva en el nivel del puerto distribuido, habilite la opción de anulación en el nivel de puerto para esta directiva. Consulte Configurar las directivas de red de anulación en los puertos.

Procedimiento

1 En vSphere Web Client, desplácese hasta el conmutador distribuido.

2 Desplácese hasta la directiva de catalogación de tráfico del puerto o del grupo de puertos distribuidos.

Opción	Acción
Grupo de puertos distribuidos	a En el menú **Acciones** seleccione **Grupo de puertos distribuidos > Administrar grupos de puertos distribuidos**. b Seleccione **Catalogación de tráfico**. c Seleccione el grupo de puertos y haga clic en **Siguiente**.
Puerto distribuido	a En la pestaña **Redes**, haga clic en **Grupos de puertos distribuidos** y, a continuación, haga doble clic en un grupo de puertos distribuidos. b En la pestaña **Puertos**, seleccione un puerto y haga clic en el icono **Editar configuración de puertos distribuidos**. c Seleccione **Catalogación de tráfico**. d Seleccione **Anular** junto a las propiedades que desea anular.

3 Configure las directivas de catalogación de tráfico.

Nota El tráfico se clasifica en tráfico de ingreso y tráfico de egreso de acuerdo con la dirección del tráfico en el conmutador, no en el host.

Opción	Descripción
Estado	Habilite **Catalogación de tráfico de ingreso** o **Catalogación de tráfico de egreso** mediante los menús desplegables **Estado**.
Ancho de banda promedio	Establece la cantidad de bits por segundo que se asignan en un puerto, promediada en el tiempo, es decir, la carga promedio permitida.

Opción	Descripción
Ancho de banda máximo	La cantidad máxima de bits por segundo que se permitirá en un puerto al enviar y/o recibir una ráfaga de tráfico. Este parámetro limita el ancho de banda utilizado por un puerto cada vez que utiliza su ráfaga adicional.
Tamaño de ráfaga	Es la cantidad máxima de bytes que se permiten en una ráfaga. Si se establece este parámetro, un puerto podría recibir una ráfaga adicional cuando no utiliza todo el ancho de banda asignado. Si el puerto necesita más ancho de banda que el promedio especificado, el puerto puede transmitir datos temporalmente a una velocidad superior si hay una ráfaga adicional disponible. Este parámetro aumenta la cantidad de bytes que se pueden acumular en la ráfaga adicional y transferir a una velocidad mayor.

4 Revise las opciones y aplique la configuración.

Directiva de asignación de recursos

La directiva de asignación de recursos permite asociar un grupo de puertos o un puerto distribuido con un grupo de recursos de red creados por el usuario. Esta directiva proporciona mayor control sobre el ancho de banda asignado al puerto o al grupo de puertos.

Para obtener información sobre cómo crear y configurar grupos de recursos de red, consulte Capítulo 11 vSphere Network I/O Control.

Editar la directiva de asignación de recursos en un grupo de puertos distribuidos

Asocie un grupo de puertos distribuidos con un grupo de recursos de red para obtener mayor control sobre el ancho de banda que recibe el grupo de puertos distribuidos.

Requisitos previos

- Habilite Network I/O Control en el conmutador distribuido. Consulte Habilitar Network I/O Control en vSphere Distributed Switch.
- Cree y configure grupos de recursos de red. Consulte Crear un grupo de recursos de red.

Procedimiento

1 En vSphere Web Client, desplácese hasta el conmutador distribuido.

2 Haga clic con el botón derecho en el conmutador distribuido del navegador y seleccione **Grupos de puertos distribuidos > Administrar grupos de puertos distribuidos**.

3 Active la casilla **Asignación de recursos** y haga clic en **Siguiente**.

4 Seleccione el grupo de puertos distribuidos que desea configurar y haga clic en **Siguiente**.

5 Agregue o quite el grupo de puertos distribuidos del grupo de recursos de red y haga clic en **Siguiente**.

   - Para agregar el grupo de puertos distribuidos, seleccione un grupo de recursos definidos por el usuario desde el menú desplegable **Grupo de recursos de red**.

- Para quitar el grupo de puertos distribuidos, seleccione **valor predeterminado** en el menú desplegable **Grupo de recursos de red**.

6 Revise la configuración en la página **Listo para finalizar** y haga clic en **Finalizar**.

  Utilice el botón **Atrás** para cambiar cualquier configuración.

Editar la directiva de asignación de recursos en un puerto distribuido

Si utiliza la versión 2 de Network I/O Control en vSphere Distributed Switch, puede asociar específicamente un puerto distribuido con un grupo de recursos definidos por el usuario a fin de utilizar Network I/O Control para que controle el ancho de banda proporcionado a la máquina virtual conectada al puerto.

Requisitos previos

- Compruebe que Network I/O Control sea la versión 2.
- Habilite Network I/O Control en el conmutador distribuido. Consulte Habilitar Network I/O Control en vSphere Distributed Switch.
- Cree y configure grupos de recursos de red en Network I/O Control versión 2. Consulte Crear un grupo de recursos de red en la versión 2 de Network I/O Control.
- Habilite anulaciones en el nivel de puerto correspondientes a la directiva de asignación de recursos. Consulte Configurar las directivas de red de anulación en los puertos.

Procedimiento

1 En vSphere Web Client, desplácese hasta el conmutador distribuido.

2 En la pestaña **Configurar**, expanda **Más** y haga clic en **Puertos**.

3 Seleccione un puerto de la lista y haga clic en el icono **Editar configuración de puertos distribuidos**.

4 Seleccione **Propiedades**.

5 En el grupo de recursos de red, active la casilla **Anular**, y en el menú desplegable asígnele al puerto un grupo de recursos de red.

  Si no habilitó las anulaciones en el nivel de puerto para la directiva de asignación de recursos, la opción está deshabilitada.

  - Para asociar el puerto distribuido a un grupo de recursos, seleccione un grupo de recursos definidos por el usuario.
  - Para quitar la asociación entre el puerto distribuido y un grupo de recursos, seleccione **valor predeterminado**.

6 Haga clic en **Aceptar**.

Directiva de supervisión

La directiva de supervisión habilita o deshabilita la supervisión de NetFlow en un puerto o un grupo de puertos distribuidos.

Las opciones de NetFlow se configuran en el nivel del conmutador distribuido de vSphere. Consulte Configurar opciones de NetFlow para vSphere Distributed Switch.

Habilitar o deshabilitar la supervisión de NetFlow en un puerto distribuido o en un grupo de puertos distribuidos

Es posible habilitar NetFlow para supervisar los paquetes IP que atraviesan los puertos de un grupo de puertos distribuidos o a través de puertos distribuidos individuales.

Es posible establecer la configuración de NetFlow en vSphere Distributed Switch. Consulte Configurar opciones de NetFlow para vSphere Distributed Switch

Requisitos previos

Para anular una directiva en el nivel del puerto distribuido, habilite la opción de anulación en el nivel de puerto para esta directiva. Consulte Configurar las directivas de red de anulación en los puertos.

Procedimiento

1 En vSphere Web Client, desplácese hasta el conmutador distribuido.

2 Desplácese hasta la directiva de supervisión correspondiente al puerto distribuido o al grupo de puertos distribuidos.

Opción	Acción
Grupo de puertos distribuidos	a En el menú **Acciones** seleccione **Grupo de puertos distribuidos > Administrar grupos de puertos distribuidos**. b Seleccione **Supervisión**. c Seleccione el grupo de puertos y haga clic en **Siguiente**.
Puerto distribuido	a En la pestaña **Redes**, haga clic en **Grupos de puertos distribuidos** y, a continuación, haga doble clic en un grupo de puertos distribuidos. b En la pestaña **Puertos**, seleccione un puerto y haga clic en el icono **Editar configuración de puertos distribuidos**. c Seleccione **Supervisión**. d Seleccione **Anular** junto a las propiedades que desea anular.

3 Habilite o deshabilite NetFlow en el menú desplegable **NetFlow** y haga clic en **Siguiente**.

4 Compruebe la configuración y aplíquela.

Directiva de filtrado y marcado de tráfico

En vSphere Distributed Switch versión 5.5 y posteriores, la directiva de filtrado y marcado de tráfico permite proteger la red virtual ante el tráfico no deseado y los ataques de seguridad o aplicar una etiqueta de QoS a un tipo de tráfico específico.

La directiva de filtrado y marcado de tráfico representa un conjunto ordenado de reglas de tráfico de red para la seguridad y el etiquetado de QoS del flujo de datos a través de los puertos de un conmutador distribuido. En general, una regla consta de un calificador para el tráfico y una acción para restringir o priorizar el tráfico que coincida con la regla.

El conmutador distribuido de vSphere aplica las reglas al tráfico en diferentes puntos del flujo de datos. El conmutador distribuido aplica las reglas de filtro de tráfico en la ruta de datos entre el adaptador de red de máquina virtual y el puerto distribuido, o entre el puerto de vínculo superior y el adaptador de red físico para las reglas de vínculos superiores.

Filtrar y marcar tráfico en un grupo de puertos distribuidos o un grupo de puertos de vínculo superior

Establezca las reglas de tráfico en el nivel de los grupos de puertos distribuidos o los grupos de puertos de vínculo superior para introducir el filtrado y el etiquetado de prioridades en el tráfico a través de máquinas virtuales, adaptadores VMkernel o adaptadores físicos.

- Habilitar el filtrado y marcado de tráfico en un grupo de puertos distribuidos o un grupo de puertos de vínculo superior

  Habilite la directiva de filtrado y marcado de tráfico en un grupo de puertos si desea configurar la seguridad y el marcado del tráfico en todos los adaptadores de red de máquina virtual o los adaptadores de vínculo superior que forman parte del grupo.

- Marcar tráfico en un grupo de puertos distribuidos o un grupo de puertos de vínculo superior

  Asigne etiquetas de prioridad al tráfico, por ejemplo a VoIP y a la transmisión de vídeo, que tenga mayores requisitos de redes respecto del ancho de banda, de la baja latencia y otras características. Puede marcar el tráfico con una etiqueta de CoS en la Capa 2 de la pila del protocolo de red o con una etiqueta de DSCP en la Capa 3.

- Filtrar tráfico en un grupo de puertos distribuidos o un grupo de puertos de vínculo superior

  Permita o interrumpa el tráfico para proteger los datos que se transmiten a través de los puertos de un grupo de puertos distribuidos o un grupo de puertos de vínculo superior.

- Trabajar con reglas de tráfico de red en un grupo de puertos distribuidos o un grupo de puertos de vínculo superior

  Defina las reglas de tráfico en un grupo de puertos distribuidos o un grupo de puertos de vínculo superior para introducir una directiva para procesar el tráfico relacionado con las máquinas virtuales o los adaptadores físicos. Se puede filtrar un tráfico específico o describir la demanda de QoS.

- Deshabilitar el filtrado y marcado de tráfico en un grupo de puertos distribuidos o un grupo de puertos de vínculo superior

  Deshabilite la directiva de filtrado y marcado de tráfico para que el tráfico fluya a las máquinas virtuales o los adaptadores físicos sin ningún control adicional de seguridad o QoS.

Habilitar el filtrado y marcado de tráfico en un grupo de puertos distribuidos o un grupo de puertos de vínculo superior

Habilite la directiva de filtrado y marcado de tráfico en un grupo de puertos si desea configurar la seguridad y el marcado del tráfico en todos los adaptadores de red de máquina virtual o los adaptadores de vínculo superior que forman parte del grupo.

Nota Puede deshabilitar la directiva de filtrado y marcado de tráfico en un puerto específico para evitar que se procese el tráfico que se transmite a través de ese puerto. Consulte Deshabilitar el filtrado y marcado de tráfico en un puerto distribuido o un puerto de vínculo superior.

Procedimiento

1 Busque un grupo de puertos distribuidos o un grupo de puertos de vínculo superior en vSphere Web Client.

   a Seleccione un conmutador distribuido y haga clic en la pestaña **Redes**.

   b Haga clic en **Grupos de puertos distribuidos** para ver la lista de puertos distribuidos o haga clic en **Grupos de puertos de vínculo superior** para ver la lista de grupos de puertos de enlace de subida.

2 Haga clic con el botón derecho en el grupo de puertos y seleccione **Editar configuración**.

3 Seleccione **Filtrado y marcado de tráfico**.

4 En el menú desplegable **Estado**, seleccione **Habilitado**.

5 Haga clic en **Aceptar**.

Pasos siguientes

Configure el marcado o el filtrado de tráfico para los datos que se transmiten a través de los puertos del grupo de puertos distribuidos o del grupo de puertos de vínculo superior. Consulte Marcar tráfico en un grupo de puertos distribuidos o un grupo de puertos de vínculo superior y Filtrar tráfico en un grupo de puertos distribuidos o un grupo de puertos de vínculo superior.

Marcar tráfico en un grupo de puertos distribuidos o un grupo de puertos de vínculo superior

Asigne etiquetas de prioridad al tráfico, por ejemplo a VoIP y a la transmisión de vídeo, que tenga mayores requisitos de redes respecto del ancho de banda, de la baja latencia y otras características. Puede marcar el tráfico con una etiqueta de CoS en la Capa 2 de la pila del protocolo de red o con una etiqueta de DSCP en la Capa 3.

El etiquetado de prioridad es un mecanismo para marcar el tráfico que tiene mayores demandas de QoS. De esta manera, la red puede reconocer diferentes clases de tráfico. Los dispositivos de red pueden controlar el tráfico de cada clase de acuerdo con su prioridad y requisitos.

El tráfico también se puede volver a etiquetar, ya sea para aumentar o para disminuir la importancia del flujo. Mediante la utilización de una etiqueta de QoS baja, se pueden restringir los datos etiquetados en un sistema operativo invitado.

Procedimiento

1 Busque un grupo de puertos distribuidos o un grupo de puertos de vínculo superior en vSphere Web Client.

   a Seleccione un conmutador distribuido y haga clic en la pestaña **Redes**.

   b Haga clic en **Grupos de puertos distribuidos** para ver la lista de puertos distribuidos o haga clic en **Grupos de puertos de vínculo superior** para ver la lista de grupos de puertos de enlace de subida.

2 Haga clic con el botón derecho en el grupo de puertos y seleccione **Editar configuración**.

3 Seleccione **Filtrado y marcado de tráfico**.

4 Si el filtrado y el marcado de tráfico están deshabilitados, habilítelos en el menú desplegable **Estado**.

5 Haga clic en **Nuevo** para crear una nueva regla o seleccione una regla y haga clic en **Editar** para editarla.

6 En el cuadro de diálogo de las reglas del tráfico de red, seleccione la opción **Etiquetar** en el menú desplegable **Acción**.

7 Establezca la etiqueta de prioridad correspondiente al tráfico dentro del alcance de la regla.

Opción	Descripción
Valor de CoS	Marque el tráfico que coincide con la regla con una etiqueta de prioridad CoS en la Capa 2 de la red. Seleccione **Actualizar etiqueta CoS** y escriba un valor entre 0 y 7.
Valor DSCP	Marque el tráfico asociado a la regla con una etiqueta DSCP en la Capa 3 de la red. Seleccione **Actualizar valor DSCP** y escriba un valor entre 0 y 63.

8 Especifique el tipo de tráfico al que se debe aplicar la regla.

Para determinar si un flujo de datos se encuentra en el ámbito de aplicación de una regla para el marcado o el filtrado, el conmutador distribuido de vSphere examina la dirección del tráfico y las propiedades como origen y destino, VLAN, protocolo de siguiente nivel, infraestructura de tipo de tráfico, entre otras.

a En el menú desplegable **Dirección del tráfico**, seleccione si el tráfico debe ser de ingreso, de egreso o de ambos, para que la regla lo reconozca como coincidente.

   La dirección también influye en la manera en que se va a identificar el origen y el destino del tráfico.

b Mediante la utilización de calificadores para el tipo de datos del sistema, los atributos del paquete de la Capa 2 y de la Capa 3, establezca las propiedades que los paquetes deben tener para coincidir con la regla.

   Un calificador representa un conjunto de criterios de coincidencia relacionados con una capa de redes. Se puede hacer coincidir el tráfico con el tipo de datos del sistema, las propiedades del tráfico de la Capa 2 y las propiedades del tráfico de la Capa 3. Se puede utilizar el calificador para una capa de redes específica, o bien se pueden combinar los calificadores para que coincidan de manera precisa con los paquetes.

   - Utilice el calificador de tráfico del sistema para que haga coincidir los paquetes con el tipo de datos de infraestructura virtual que está fluyendo a través de los puertos del grupo. Por ejemplo, se puede seleccionar NFS para las transferencias de datos al almacenamiento de red.
   - Utilice el calificador de tráfico MAC para hacer coincidir los paquetes por la dirección MAC, el identificador de VLAN y el protocolo de siguiente nivel.

     La localización de tráfico con un identificador de VLAN en un grupo de puertos distribuidos funciona con el etiquetado de invitado virtual (VGT). Para que el tráfico coincida con el identificador de VLAN si el etiquetado de conmutador virtual (VST) está activo, utilice una regla en un grupo de puertos de vínculo superior o en un puerto de vínculo superior.
   - Utilice el calificador de tráfico IP para que los paquetes coincidan por la versión IP, la dirección IP, y el puerto y el protocolo de siguiente nivel.

9 En el cuadro de diálogo de la regla, haga clic en **Aceptar** para guardar la regla.

Ejemplo: Marcado del tráfico de voz sobre IP

Los flujos de voz sobre IP (VoIP) tienen requisitos especiales de QoS en cuanto al bajo nivel de pérdida y de retraso. El tráfico relacionado con el protocolo Session Initiation Protocol (SIP) para VoIP generalmente tiene una etiqueta de DSCP equivalente a 26, que representa la clase de reenvío garantizado 3 (Assured Forwarding Class, AF31) con baja probabilidad de descarte.

Por ejemplo, para marcar los paquetes UDP de SIP salientes a una subred 192.168.2.0/24, puede utilizar la siguiente regla:

Parámetro de regla	Valor del parámetro
Acción	Etiquetar
Valor DSCP	26
Dirección del tráfico	Egreso
Calificadores de tráfico	Calificador de IP
Protocolo	UDP
Puerto de destino	5060
Dirección de origen	La dirección IP coincide con 192.168.2.0 con la longitud de prefijo 24

Filtrar tráfico en un grupo de puertos distribuidos o un grupo de puertos de vínculo superior

Permita o interrumpa el tráfico para proteger los datos que se transmiten a través de los puertos de un grupo de puertos distribuidos o un grupo de puertos de vínculo superior.

Procedimiento

1 Busque un grupo de puertos distribuidos o un grupo de puertos de vínculo superior en vSphere Web Client.

   a Seleccione un conmutador distribuido y haga clic en la pestaña **Redes**.

   b Haga clic en **Grupos de puertos distribuidos** para ver la lista de puertos distribuidos o haga clic en **Grupos de puertos de vínculo superior** para ver la lista de grupos de puertos de enlace de subida.

2 Haga clic con el botón derecho en el grupo de puertos y seleccione **Editar configuración**.

3 Seleccione **Filtrado y marcado de tráfico**.

4 Si el filtrado y el marcado de tráfico están deshabilitados, habilítelos en el menú desplegable **Estado**.

5 Haga clic en **Nuevo** para crear una nueva regla o seleccione una regla y haga clic en **Editar** para editarla.

6 En el cuadro de diálogo de regla de tráfico de red, use las opciones de la sección Acción para permitir el tráfico por los puertos del grupo de puertos distribuidos o del grupo de puertos de vínculo superior, o para restringir el tráfico.

7 Especifique el tipo de tráfico al que se debe aplicar la regla.

Para determinar si un flujo de datos se encuentra en el ámbito de aplicación de una regla para el marcado o el filtrado, el conmutador distribuido de vSphere examina la dirección del tráfico y las propiedades como origen y destino, VLAN, protocolo de siguiente nivel, infraestructura de tipo de tráfico, entre otras.

a En el menú desplegable **Dirección del tráfico**, seleccione si el tráfico debe ser de ingreso, de egreso o de ambos, para que la regla lo reconozca como coincidente.

   La dirección también influye en la manera en que se va a identificar el origen y el destino del tráfico.

b Mediante la utilización de calificadores para el tipo de datos del sistema, los atributos del paquete de la Capa 2 y de la Capa 3, establezca las propiedades que los paquetes deben tener para coincidir con la regla.

   Un calificador representa un conjunto de criterios de coincidencia relacionados con una capa de redes. Se puede hacer coincidir el tráfico con el tipo de datos del sistema, las propiedades del tráfico de la Capa 2 y las propiedades del tráfico de la Capa 3. Se puede utilizar el calificador para una capa de redes específica, o bien se pueden combinar los calificadores para que coincidan de manera precisa con los paquetes.

   - Utilice el calificador de tráfico del sistema para que haga coincidir los paquetes con el tipo de datos de infraestructura virtual que está fluyendo a través de los puertos del grupo. Por ejemplo, se puede seleccionar NFS para las transferencias de datos al almacenamiento de red.
   - Utilice el calificador de tráfico MAC para hacer coincidir los paquetes por la dirección MAC, el identificador de VLAN y el protocolo de siguiente nivel.

     La localización de tráfico con un identificador de VLAN en un grupo de puertos distribuidos funciona con el etiquetado de invitado virtual (VGT). Para que el tráfico coincida con el identificador de VLAN si el etiquetado de conmutador virtual (VST) está activo, utilice una regla en un grupo de puertos de vínculo superior o en un puerto de vínculo superior.
   - Utilice el calificador de tráfico IP para que los paquetes coincidan por la versión IP, la dirección IP, y el puerto y el protocolo de siguiente nivel.

8 En el cuadro de diálogo de la regla, haga clic en **Aceptar** para guardar la regla.

Trabajar con reglas de tráfico de red en un grupo de puertos distribuidos o un grupo de puertos de vínculo superior

Defina las reglas de tráfico en un grupo de puertos distribuidos o un grupo de puertos de vínculo superior para introducir una directiva para procesar el tráfico relacionado con las máquinas

virtuales o los adaptadores físicos. Se puede filtrar un tráfico específico o describir la demanda de QoS.

Nota Se pueden anular las reglas de la directiva para el marcado y el filtrado del tráfico en el nivel de puerto. Consulte Trabajar con reglas de tráfico de red en un puerto distribuido o un puerto de vínculo superior.

- Ver reglas de tráfico en un grupo de puertos distribuidos o un grupo de vínculo superior

  Vea las reglas de tráfico que conforman la directiva de filtrado y marcado de tráfico de un grupo de puertos distribuidos o de un grupo de puertos de vínculo superior.

- Editar una regla de tráfico en un grupo de puertos distribuidos o un grupo de puertos de vínculo superior

  Cree o edite reglas de tráfico y utilice sus parámetros para configurar una directiva para filtrar o marcar el tráfico en un grupo de puertos distribuidos o un grupo de puertos de vínculo superior.

- Cambiar las prioridades de reglas en un grupo de puertos distribuidos o un grupo de puertos de vínculo superior

  Reorganice las reglas que conforman la directiva de filtrado y marcado de tráfico de un grupo de puertos distribuidos o un grupo de puertos de vínculo superior si desea cambiar la secuencia de las acciones de procesamiento de tráfico.

- Eliminar una regla de tráfico en un grupo de puertos distribuidos o un grupo de puertos de vínculo superior

  Elimine una regla de tráfico en un grupo de puertos distribuidos o un grupo de puertos de vínculo superior para detener el procesamiento de paquetes que fluyen de una manera específica a las máquinas virtuales o a los adaptadores físicos.

Ver reglas de tráfico en un grupo de puertos distribuidos o un grupo de vínculo superior

Vea las reglas de tráfico que conforman la directiva de filtrado y marcado de tráfico de un grupo de puertos distribuidos o de un grupo de puertos de vínculo superior.

Procedimiento

1 Busque un grupo de puertos distribuidos o un grupo de puertos de vínculo superior en vSphere Web Client.

   a Seleccione un conmutador distribuido y haga clic en la pestaña **Redes**.

   b Haga clic en **Grupos de puertos distribuidos** para ver la lista de puertos distribuidos o haga clic en **Grupos de puertos de vínculo superior** para ver la lista de grupos de puertos de enlace de subida.

2 Haga clic con el botón derecho en el grupo de puertos y seleccione **Editar configuración**.

3 Seleccione **Filtrado y marcado de tráfico**.

4. Si el filtrado y el marcado de tráfico están deshabilitados, habilítelos en el menú desplegable **Estado**.
5. Examine **Acción** para determinar si la regla filtra el tráfico (permitir o denegar) o marca el tráfico (etiquetar) con demandas especiales de QoS.
6. De la lista superior, seleccione la regla para la que desea ver los criterios para la localización del tráfico.

   Los parámetros de calificación del tráfico de la regla aparecen en la lista Calificadores de tráfico.

Editar una regla de tráfico en un grupo de puertos distribuidos o un grupo de puertos de vínculo superior

Cree o edite reglas de tráfico y utilice sus parámetros para configurar una directiva para filtrar o marcar el tráfico en un grupo de puertos distribuidos o un grupo de puertos de vínculo superior.

Procedimiento

1. Busque un grupo de puertos distribuidos o un grupo de puertos de vínculo superior en vSphere Web Client.
   a. Seleccione un conmutador distribuido y haga clic en la pestaña **Redes**.
   b. Haga clic en **Grupos de puertos distribuidos** para ver la lista de puertos distribuidos o haga clic en **Grupos de puertos de vínculo superior** para ver la lista de grupos de puertos de enlace de subida.
2. Haga clic con el botón derecho en el grupo de puertos y seleccione **Editar configuración**.
3. Seleccione **Filtrado y marcado de tráfico**.
4. Si el filtrado y el marcado de tráfico están deshabilitados, habilítelos en el menú desplegable **Estado**.
5. Haga clic en **Nuevo** para crear una nueva regla o seleccione una regla y haga clic en **Editar** para editarla.

Pasos siguientes

Asígnele un nombre a la regla de tráfico de la red y etiquete, permita o niegue el tráfico de destino.

Cambiar las prioridades de reglas en un grupo de puertos distribuidos o un grupo de puertos de vínculo superior

Reorganice las reglas que conforman la directiva de filtrado y marcado de tráfico de un grupo de puertos distribuidos o un grupo de puertos de vínculo superior si desea cambiar la secuencia de las acciones de procesamiento de tráfico.

El conmutador distribuido de vSphere aplica reglas de tráfico de red en un orden estricto. Si un paquete ya cumple una regla, es posible que este no pueda pasarse a la siguiente regla de la directiva.

Procedimiento

1 Busque un grupo de puertos distribuidos o un grupo de puertos de vínculo superior en vSphere Web Client.

   a Seleccione un conmutador distribuido y haga clic en la pestaña **Redes**.

   b Haga clic en **Grupos de puertos distribuidos** para ver la lista de puertos distribuidos o haga clic en **Grupos de puertos de vínculo superior** para ver la lista de grupos de puertos de enlace de subida.

2 Haga clic con el botón derecho en el grupo de puertos y seleccione **Editar configuración**.

3 Seleccione **Filtrado y marcado de tráfico**.

4 Si el filtrado y el marcado de tráfico están deshabilitados, habilítelos en el menú desplegable **Estado**.

5 Seleccione una regla y utilice los botones de flecha para cambiar su prioridad.

6 Haga clic en **Aceptar** para aplicar los cambios.

Eliminar una regla de tráfico en un grupo de puertos distribuidos o un grupo de puertos de vínculo superior

Elimine una regla de tráfico en un grupo de puertos distribuidos o un grupo de puertos de vínculo superior para detener el procesamiento de paquetes que fluyen de una manera específica a las máquinas virtuales o a los adaptadores físicos.

Procedimiento

1 Busque un grupo de puertos distribuidos o un grupo de puertos de vínculo superior en vSphere Web Client.

   a Seleccione un conmutador distribuido y haga clic en la pestaña **Redes**.

   b Haga clic en **Grupos de puertos distribuidos** para ver la lista de puertos distribuidos o haga clic en **Grupos de puertos de vínculo superior** para ver la lista de grupos de puertos de enlace de subida.

2 Haga clic con el botón derecho en el grupo de puertos y seleccione **Editar configuración**.

3 Seleccione **Filtrado y marcado de tráfico**.

4 Si el filtrado y el marcado de tráfico están deshabilitados, habilítelos en el menú desplegable **Estado**.

5 Seleccione la regla y haga clic en **Eliminar**.

6 Haga clic en **Aceptar**.

Deshabilitar el filtrado y marcado de tráfico en un grupo de puertos distribuidos o un grupo de puertos de vínculo superior

Deshabilite la directiva de filtrado y marcado de tráfico para que el tráfico fluya a las máquinas virtuales o los adaptadores físicos sin ningún control adicional de seguridad o QoS.

Nota Puede habilitar y configurar la directiva de filtrado y marcado de tráfico en un puerto específico. Consulte Habilitar el marcado y el filtrado de tráfico en un puerto distribuido o en un puerto de vínculo superior.

Procedimiento

1 Busque un grupo de puertos distribuidos o un grupo de puertos de vínculo superior en vSphere Web Client.

   a Seleccione un conmutador distribuido y haga clic en la pestaña **Redes**.

   b Haga clic en **Grupos de puertos distribuidos** para ver la lista de puertos distribuidos o haga clic en **Grupos de puertos de vínculo superior** para ver la lista de grupos de puertos de enlace de subida.

2 Haga clic con el botón derecho en el grupo de puertos y seleccione **Editar configuración**.

3 Seleccione **Filtrado y marcado de tráfico**.

4 En el menú desplegable **Estado**, seleccione **Deshabilitado**.

5 Haga clic en **Aceptar**.

Filtrar y marcar de tráfico en un puerto distribuido o un puerto de vínculo superior

Para filtrar el tráfico o describir las exigencias de QoS para una máquina virtual, un adaptador VMkernel o un adaptador físico individual, configure la directiva de filtrado y marcado de tráfico en un puerto distribuido o puerto de vínculo superior.

- Habilitar el marcado y el filtrado de tráfico en un puerto distribuido o en un puerto de vínculo superior

  Habilite la directiva de marcado y filtrado de tráfico en un puerto para configurar la seguridad del tráfico y la señalización en un adaptador de red de máquina virtual, un adaptador VMkernel o un adaptador de vínculo superior.

- Marcar tráfico en un puerto distribuido o un puerto de vínculo superior

  Asigne etiquetas de prioridad en una regla para el tráfico que requiera tratamiento especial, como VoIP y transmisión de vídeo. Puede marcar el tráfico de una máquina virtual, adaptador VMkernel o adaptador físico con una etiqueta de CoS en la Capa 2 de la pila del protocolo de red o con una etiqueta de DSCP en la Capa 3.

- Filtrar tráfico en un puerto distribuido o un puerto de vínculo superior

  Use las reglas para permitir o detener el tráfico a fin de proteger los flujos de datos que pasan por una máquina virtual, un adaptador VMkernel o un adaptador físico.

- Trabajar con reglas de tráfico de red en un puerto distribuido o un puerto de vínculo superior

  Defina las reglas de tráfico en un grupo de puertos distribuidos o puertos de vínculo superior para introducir una directiva de procesamiento del tráfico relacionado con una máquina virtual o un adaptador físico. Se puede filtrar un tráfico específico o describir la demanda de QoS.

- Deshabilitar el filtrado y marcado de tráfico en un puerto distribuido o un puerto de vínculo superior

  Deshabilite la directiva de filtrado y marcado de tráfico en un puerto para permitir que el tráfico pase por una máquina virtual o un adaptador físico sin filtrado de seguridad o marcado de QoS.

Habilitar el marcado y el filtrado de tráfico en un puerto distribuido o en un puerto de vínculo superior

Habilite la directiva de marcado y filtrado de tráfico en un puerto para configurar la seguridad del tráfico y la señalización en un adaptador de red de máquina virtual, un adaptador VMkernel o un adaptador de vínculo superior.

Requisitos previos

Para anular una directiva en el nivel del puerto distribuido, habilite la opción de anulación en el nivel de puerto para esta directiva. Consulte Configurar las directivas de red de anulación en los puertos.

Procedimiento

1 Desplácese hasta un conmutador distribuido y después hasta un puerto distribuido o un puerto de vínculo superior.

   - Para desplazarse hasta los puertos distribuidos del conmutador, haga clic en **Redes > Grupos de puertos distribuidos**, haga doble clic en un grupo de puertos distribuidos de la lista y, a continuación, haga clic en la pestaña **Puertos**.
   - Para desplazarse hasta los puertos de vínculo superior de un grupo de puertos de vínculo superior, haga clic en **Redes > Grupos de puertos de vínculo superior**, haga doble clic en un grupo de puertos de vínculo superior de la lista y, a continuación, haga clic en la pestaña **Puertos**.

2 Seleccione un puerto de la lista.

3 Haga clic en **Editar configuración de puertos distribuidos**.

4 Seleccione **Filtrado y marcado de tráfico**.

5 Active la casilla **Anular** y en el menú desplegable **Estado**, seleccione **Habilitado**.

6 Haga clic en **Aceptar**.

Pasos siguientes

Establezca el marcado o el filtrado de tráfico correspondientes a los datos que fluyen a través del puerto distribuido o a través del puerto de vínculo superior. Consulte Marcar tráfico en un puerto distribuido o un puerto de vínculo superior y Filtrar tráfico en un puerto distribuido o un puerto de vínculo superior.

Marcar tráfico en un puerto distribuido o un puerto de vínculo superior

Asigne etiquetas de prioridad en una regla para el tráfico que requiera tratamiento especial, como VoIP y transmisión de vídeo. Puede marcar el tráfico de una máquina virtual, adaptador VMkernel o adaptador físico con una etiqueta de CoS en la Capa 2 de la pila del protocolo de red o con una etiqueta de DSCP en la Capa 3.

El etiquetado de prioridad es un mecanismo para marcar el tráfico que tiene mayores demandas de QoS. De esta manera, la red puede reconocer diferentes clases de tráfico. Los dispositivos de red pueden controlar el tráfico de cada clase de acuerdo con su prioridad y requisitos.

El tráfico también se puede volver a etiquetar, ya sea para aumentar o para disminuir la importancia del flujo. Mediante la utilización de una etiqueta de QoS baja, se pueden restringir los datos etiquetados en un sistema operativo invitado.

Requisitos previos

Para anular una directiva en el nivel del puerto distribuido, habilite la opción de anulación en el nivel de puerto para esta directiva. Consulte Configurar las directivas de red de anulación en los puertos.

Procedimiento

1 Desplácese hasta un conmutador distribuido y después hasta un puerto distribuido o un puerto de vínculo superior.

   - Para desplazarse hasta los puertos distribuidos del conmutador, haga clic en **Redes > Grupos de puertos distribuidos**, haga doble clic en un grupo de puertos distribuidos de la lista y, a continuación, haga clic en la pestaña **Puertos**.
   - Para desplazarse hasta los puertos de vínculo superior de un grupo de puertos de vínculo superior, haga clic en **Redes > Grupos de puertos de vínculo superior**, haga doble clic en un grupo de puertos de vínculo superior de la lista y, a continuación, haga clic en la pestaña **Puertos**.

2 Seleccione un puerto de la lista.

3 Haga clic en **Editar configuración de puertos distribuidos**.

4 Si el filtrado y el marcado de tráfico no está habilitado en el nivel de puerto, haga clic en **Anular**, y en el menú desplegable **Estado**, seleccione **Habilitado**.

5 Haga clic en **Nuevo** para crear una nueva regla o seleccione una regla y haga clic en **Editar** para editarla.

   Se puede cambiar una regla heredada del grupo de puertos distribuidos o del grupo de puertos de vínculo superior. De esta manera, la regla se vuelve exclusiva dentro del alcance del puerto.

6 En el cuadro de diálogo de las reglas del tráfico de red, seleccione la opción **Etiquetar** en el menú desplegable **Acción**.

7 Establezca la etiqueta de prioridad correspondiente al tráfico dentro del alcance de la regla.

Opción	Descripción
Valor de CoS	Marque el tráfico que coincide con la regla con una etiqueta de prioridad CoS en la Capa 2 de la red. Seleccione **Actualizar etiqueta CoS** y escriba un valor entre 0 y 7.
Valor DSCP	Marque el tráfico asociado a la regla con una etiqueta DSCP en la Capa 3 de la red. Seleccione **Actualizar valor DSCP** y escriba un valor entre 0 y 63.

8 Especifique el tipo de tráfico al que se debe aplicar la regla.

Para determinar si un flujo de datos se encuentra en el ámbito de aplicación de una regla para el marcado o el filtrado, el conmutador distribuido de vSphere examina la dirección del tráfico y las propiedades como origen y destino, VLAN, protocolo de siguiente nivel, infraestructura de tipo de tráfico, entre otras.

a En el menú desplegable **Dirección del tráfico**, seleccione si el tráfico debe ser de ingreso, de egreso o de ambos, para que la regla lo reconozca como coincidente.

   La dirección también influye en la manera en que se va a identificar el origen y el destino del tráfico.

b Mediante la utilización de calificadores para el tipo de datos del sistema, los atributos del paquete de la Capa 2 y de la Capa 3, establezca las propiedades que los paquetes deben tener para coincidir con la regla.

   Un calificador representa un conjunto de criterios de coincidencia relacionados con una capa de redes. Se puede hacer coincidir el tráfico con el tipo de datos del sistema, las propiedades del tráfico de la Capa 2 y las propiedades del tráfico de la Capa 3. Se puede utilizar el calificador para una capa de redes específica, o bien se pueden combinar los calificadores para que coincidan de manera precisa con los paquetes.

   - Utilice el calificador de tráfico del sistema para que haga coincidir los paquetes con el tipo de datos de infraestructura virtual que está fluyendo a través de los puertos del grupo. Por ejemplo, se puede seleccionar NFS para las transferencias de datos al almacenamiento de red.
   - Utilice el calificador de tráfico MAC para hacer coincidir los paquetes por la dirección MAC, el identificador de VLAN y el protocolo de siguiente nivel.

     La localización de tráfico con un identificador de VLAN en un grupo de puertos distribuidos funciona con el etiquetado de invitado virtual (VGT). Para que el tráfico coincida con el identificador de VLAN si el etiquetado de conmutador virtual (VST) está activo, utilice una regla en un grupo de puertos de vínculo superior o en un puerto de vínculo superior.
   - Utilice el calificador de tráfico IP para que los paquetes coincidan por la versión IP, la dirección IP, y el puerto y el protocolo de siguiente nivel.

9 En el cuadro de diálogo de la regla, haga clic en **Aceptar** para guardar la regla.

Filtrar tráfico en un puerto distribuido o un puerto de vínculo superior

Use las reglas para permitir o detener el tráfico a fin de proteger los flujos de datos que pasan por una máquina virtual, un adaptador VMkernel o un adaptador físico.

Requisitos previos

Para anular una directiva en el nivel del puerto distribuido, habilite la opción de anulación en el nivel de puerto para esta directiva. Consulte Configurar las directivas de red de anulación en los puertos.

Procedimiento

1 Desplácese hasta un conmutador distribuido y después hasta un puerto distribuido o un puerto de vínculo superior.

   - Para desplazarse hasta los puertos distribuidos del conmutador, haga clic en **Redes > Grupos de puertos distribuidos**, haga doble clic en un grupo de puertos distribuidos de la lista y, a continuación, haga clic en la pestaña **Puertos**.
   - Para desplazarse hasta los puertos de vínculo superior de un grupo de puertos de vínculo superior, haga clic en **Redes > Grupos de puertos de vínculo superior**, haga doble clic en un grupo de puertos de vínculo superior de la lista y, a continuación, haga clic en la pestaña **Puertos**.

2 Seleccione un puerto de la lista.

3 Haga clic en **Editar configuración de puertos distribuidos**.

4 Si el filtrado y el marcado de tráfico no está habilitado en el nivel de puerto, haga clic en **Anular**, y en el menú desplegable **Estado**, seleccione **Habilitado**.

5 Haga clic en **Nuevo** para crear una nueva regla o seleccione una regla y haga clic en **Editar** para editarla.

   Se puede cambiar una regla heredada del grupo de puertos distribuidos o del grupo de puertos de vínculo superior. De esta manera, la regla se vuelve exclusiva dentro del alcance del puerto.

6 En el cuadro de diálogo de la regla de tráfico de red, seleccione la acción **Permitir** para dejar que el tráfico pase por el puerto distribuido o el puerto de vínculo superior, o la acción **Descartar** para restringirlo.

7 Especifique el tipo de tráfico al que se debe aplicar la regla.

Para determinar si un flujo de datos se encuentra en el ámbito de aplicación de una regla para el marcado o el filtrado, el conmutador distribuido de vSphere examina la dirección del tráfico y las propiedades como origen y destino, VLAN, protocolo de siguiente nivel, infraestructura de tipo de tráfico, entre otras.

a En el menú desplegable **Dirección del tráfico**, seleccione si el tráfico debe ser de ingreso, de egreso o de ambos, para que la regla lo reconozca como coincidente.

   La dirección también influye en la manera en que se va a identificar el origen y el destino del tráfico.

b Mediante la utilización de calificadores para el tipo de datos del sistema, los atributos del paquete de la Capa 2 y de la Capa 3, establezca las propiedades que los paquetes deben tener para coincidir con la regla.

   Un calificador representa un conjunto de criterios de coincidencia relacionados con una capa de redes. Se puede hacer coincidir el tráfico con el tipo de datos del sistema, las propiedades del tráfico de la Capa 2 y las propiedades del tráfico de la Capa 3. Se puede utilizar el calificador para una capa de redes específica, o bien se pueden combinar los calificadores para que coincidan de manera precisa con los paquetes.

   - Utilice el calificador de tráfico del sistema para que haga coincidir los paquetes con el tipo de datos de infraestructura virtual que está fluyendo a través de los puertos del grupo. Por ejemplo, se puede seleccionar NFS para las transferencias de datos al almacenamiento de red.
   - Utilice el calificador de tráfico MAC para hacer coincidir los paquetes por la dirección MAC, el identificador de VLAN y el protocolo de siguiente nivel.

     La localización de tráfico con un identificador de VLAN en un grupo de puertos distribuidos funciona con el etiquetado de invitado virtual (VGT). Para que el tráfico coincida con el identificador de VLAN si el etiquetado de conmutador virtual (VST) está activo, utilice una regla en un grupo de puertos de vínculo superior o en un puerto de vínculo superior.
   - Utilice el calificador de tráfico IP para que los paquetes coincidan por la versión IP, la dirección IP, y el puerto y el protocolo de siguiente nivel.

8 En el cuadro de diálogo de la regla, haga clic en **Aceptar** para guardar la regla.

Trabajar con reglas de tráfico de red en un puerto distribuido o un puerto de vínculo superior

Defina las reglas de tráfico en un grupo de puertos distribuidos o puertos de vínculo superior para introducir una directiva de procesamiento del tráfico relacionado con una máquina virtual o un adaptador físico. Se puede filtrar un tráfico específico o describir la demanda de QoS.

- Ver las reglas de tráfico en un puerto distribuido o en un puerto de vínculo superior

  Revise las reglas de tráfico que conforman la directiva de marcado y filtrado de tráfico de un puerto distribuido o de un puerto de vínculo superior.

- Editar una regla de tráfico en un puerto distribuido o un puerto de vínculo superior

  Cree o edite reglas de tráfico y utilice sus parámetros para configurar una directiva para filtrar o marcar el tráfico en un puerto distribuido o en un puerto de vínculo superior.

- Cambiar prioridades de reglas en un puerto distribuido o un puerto de vínculo superior

  Reorganice las reglas que conforman la directiva de filtrado y marcado de tráfico de un puerto distribuido o un puerto de vínculo superior si desea cambiar la secuencia de las acciones de análisis de tráfico para las funciones de seguridad y QoS.

- Eliminar una regla de tráfico en un puerto distribuido o en un puerto de vínculo superior

  Elimine una regla de tráfico en un puerto distribuido o en un puerto de vínculo superior para dejar de filtrar o de marcar cierto tipo de paquetes que están fluyendo hacia una máquina virtual o hacia un adaptador físico.

Ver las reglas de tráfico en un puerto distribuido o en un puerto de vínculo superior

Revise las reglas de tráfico que conforman la directiva de marcado y filtrado de tráfico de un puerto distribuido o de un puerto de vínculo superior.

Requisitos previos

Para anular una directiva en el nivel del puerto distribuido, habilite la opción de anulación en el nivel de puerto para esta directiva. Consulte Configurar las directivas de red de anulación en los puertos.

Procedimiento

1. Desplácese hasta un conmutador distribuido y después hasta un puerto distribuido o un puerto de vínculo superior.

   - Para desplazarse hasta los puertos distribuidos del conmutador, haga clic en **Redes > Grupos de puertos distribuidos**, haga doble clic en un grupo de puertos distribuidos de la lista y, a continuación, haga clic en la pestaña **Puertos**.
   - Para desplazarse hasta los puertos de vínculo superior de un grupo de puertos de vínculo superior, haga clic en **Redes > Grupos de puertos de vínculo superior**, haga doble clic en un grupo de puertos de vínculo superior de la lista y, a continuación, haga clic en la pestaña **Puertos**.

2. Seleccione un puerto de la lista.
3. Haga clic en **Editar configuración de puertos distribuidos**.
4. Seleccione **Filtrado y marcado de tráfico**.
5. Si el filtrado y el marcado de tráfico no está habilitado en el nivel de puerto, haga clic en **Anular**, y en el menú desplegable **Estado**, seleccione **Habilitado**.
6. Examine **Acción** para determinar si la regla filtra el tráfico (permitir o denegar) o marca el tráfico (etiquetar) con demandas especiales de QoS.

7 De la lista superior, seleccione la regla para la que desea ver los criterios para la localización del tráfico.

   Los parámetros de calificación del tráfico de la regla aparecen en la lista Calificadores de tráfico.

Editar una regla de tráfico en un puerto distribuido o un puerto de vínculo superior

Cree o edite reglas de tráfico y utilice sus parámetros para configurar una directiva para filtrar o marcar el tráfico en un puerto distribuido o en un puerto de vínculo superior.

Requisitos previos

Para anular una directiva en el nivel del puerto distribuido, habilite la opción de anulación en el nivel de puerto para esta directiva. Consulte Configurar las directivas de red de anulación en los puertos.

Procedimiento

1 Desplácese hasta un conmutador distribuido y después hasta un puerto distribuido o un puerto de vínculo superior.

   - Para desplazarse hasta los puertos distribuidos del conmutador, haga clic en **Redes > Grupos de puertos distribuidos**, haga doble clic en un grupo de puertos distribuidos de la lista y, a continuación, haga clic en la pestaña **Puertos**.
   - Para desplazarse hasta los puertos de vínculo superior de un grupo de puertos de vínculo superior, haga clic en **Redes > Grupos de puertos de vínculo superior**, haga doble clic en un grupo de puertos de vínculo superior de la lista y, a continuación, haga clic en la pestaña **Puertos**.

2 Seleccione un puerto de la lista.

3 Haga clic en **Editar configuración de puertos distribuidos**.

4 Seleccione **Filtrado y marcado de tráfico**.

5 Si el filtrado y el marcado de tráfico no está habilitado en el nivel de puerto, haga clic en **Anular**, y en el menú desplegable **Estado**, seleccione **Habilitado**.

6 Haga clic en **Nuevo** para crear una nueva regla o seleccione una regla y haga clic en **Editar** para editarla.

   Se puede cambiar una regla heredada del grupo de puertos distribuidos o del grupo de puertos de vínculo superior. De esta manera, la regla se vuelve exclusiva dentro del alcance del puerto.

Pasos siguientes

Asígnele un nombre a la regla de tráfico de la red y etiquete, permita o niegue el tráfico de destino.

Cambiar prioridades de reglas en un puerto distribuido o un puerto de vínculo superior

Reorganice las reglas que conforman la directiva de filtrado y marcado de tráfico de un puerto distribuido o un puerto de vínculo superior si desea cambiar la secuencia de las acciones de análisis de tráfico para las funciones de seguridad y QoS.

El conmutador distribuido de vSphere aplica reglas de tráfico de red en un orden estricto. Si un paquete ya cumple una regla, es posible que este no pueda pasarse a la siguiente regla de la directiva.

Requisitos previos

Para anular una directiva en el nivel del puerto distribuido, habilite la opción de anulación en el nivel de puerto para esta directiva. Consulte Configurar las directivas de red de anulación en los puertos.

Procedimiento

1. Desplácese hasta un conmutador distribuido y después hasta un puerto distribuido o un puerto de vínculo superior.
   - Para desplazarse hasta los puertos distribuidos del conmutador, haga clic en **Redes > Grupos de puertos distribuidos**, haga doble clic en un grupo de puertos distribuidos de la lista y, a continuación, haga clic en la pestaña **Puertos**.
   - Para desplazarse hasta los puertos de vínculo superior de un grupo de puertos de vínculo superior, haga clic en **Redes > Grupos de puertos de vínculo superior**, haga doble clic en un grupo de puertos de vínculo superior de la lista y, a continuación, haga clic en la pestaña **Puertos**.
2. Seleccione un puerto de la lista.
3. Haga clic en **Editar configuración de puertos distribuidos**.
4. Seleccione **Filtrado y marcado de tráfico**.
5. Si el filtrado y el marcado de tráfico no está habilitado en el nivel de puerto, haga clic en **Anular**, y en el menú desplegable **Estado**, seleccione **Habilitado**.
6. Seleccione una regla y utilice los botones de flecha para cambiar su prioridad.
7. Haga clic en **Aceptar** para aplicar los cambios.

Eliminar una regla de tráfico en un puerto distribuido o en un puerto de vínculo superior

Elimine una regla de tráfico en un puerto distribuido o en un puerto de vínculo superior para dejar de filtrar o de marcar cierto tipo de paquetes que están fluyendo hacia una máquina virtual o hacia un adaptador físico.

Requisitos previos

Para anular una directiva en el nivel del puerto distribuido, habilite la opción de anulación en el nivel de puerto para esta directiva. Consulte Configurar las directivas de red de anulación en los puertos.

Procedimiento

1 Desplácese hasta un conmutador distribuido y después hasta un puerto distribuido o un puerto de vínculo superior.

- Para desplazarse hasta los puertos distribuidos del conmutador, haga clic en **Redes > Grupos de puertos distribuidos**, haga doble clic en un grupo de puertos distribuidos de la lista y, a continuación, haga clic en la pestaña **Puertos**.
- Para desplazarse hasta los puertos de vínculo superior de un grupo de puertos de vínculo superior, haga clic en **Redes > Grupos de puertos de vínculo superior**, haga doble clic en un grupo de puertos de vínculo superior de la lista y, a continuación, haga clic en la pestaña **Puertos**.

2 Seleccione un puerto de la lista.

3 Haga clic en **Editar configuración de puertos distribuidos**.

4 Seleccione **Filtrado y marcado de tráfico**.

5 Si el filtrado y el marcado de tráfico no está habilitado en el nivel de puerto, haga clic en **Anular**, y en el menú desplegable **Estado**, seleccione **Habilitado**.

6 Seleccione la regla y haga clic en **Eliminar**.

7 Haga clic en **Aceptar**.

Deshabilitar el filtrado y marcado de tráfico en un puerto distribuido o un puerto de vínculo superior

Deshabilite la directiva de filtrado y marcado de tráfico en un puerto para permitir que el tráfico pase por una máquina virtual o un adaptador físico sin filtrado de seguridad o marcado de QoS.

Requisitos previos

Para anular una directiva en el nivel del puerto distribuido, habilite la opción de anulación en el nivel de puerto para esta directiva. Consulte Configurar las directivas de red de anulación en los puertos.

Procedimiento

1 Desplácese hasta un conmutador distribuido y después hasta un puerto distribuido o un puerto de vínculo superior.

- Para desplazarse hasta los puertos distribuidos del conmutador, haga clic en **Redes > Grupos de puertos distribuidos**, haga doble clic en un grupo de puertos distribuidos de la lista y, a continuación, haga clic en la pestaña **Puertos**.
- Para desplazarse hasta los puertos de vínculo superior de un grupo de puertos de vínculo superior, haga clic en **Redes > Grupos de puertos de vínculo superior**, haga doble clic en un grupo de puertos de vínculo superior de la lista y, a continuación, haga clic en la pestaña **Puertos**.

2 Seleccione un puerto de la lista.

3 Haga clic en **Editar configuración de puertos distribuidos**.

4 Seleccione **Filtrado y marcado de tráfico**.

5 Haga clic en **Anular** y, en el menú desplegable **Estado**, seleccione **Deshabilitado**.

6 Haga clic en **Aceptar**.

Calificar tráfico para filtrado y marcado

El tráfico que se desea filtrar o marcar con etiquetas de QoS se puede relacionar con el tipo de datos de infraestructura transportados, como los datos de almacenamiento, de administración de vCenter Server, etc., y con las propiedades de la Capa 2 y la Capa 3.

Para hacer que el tráfico coincida de manera más precisa con el alcance de la regla, se pueden combinar criterios para el tipo de datos del sistema, el encabezado de Capa 2 y el encabezado de Capa 3.

Calificador de tráfico del sistema

Al utilizar el calificador de tráfico del sistema en una regla para un puerto o un grupo de puertos, puede especificar si un determinado tráfico de datos del sistema debe marcase con una etiqueta de QoS, debe permitirse o debe descartarse.

Tipo de tráfico del sistema

Puede seleccionar el tipo de tráfico que pasará por los puertos del grupo que transmite los datos del sistema, es decir, el tráfico para la administración desde vCenter Server, el almacenamiento, VMware vSphere® vMotion® y vSphere Fault Tolerance. Puede marcar o filtrar solo un tipo de tráfico específico o todo el tráfico de datos del sistema, excepto una característica de infraestructura. Por ejemplo, puede marcar con un valor de QoS o filtrar el tráfico de administración desde vCenter Server, el almacenamiento y vMotion, pero no el tráfico que transporta los datos de Fault Tolerance.

Calificador de tráfico de MAC

Utilizar el calificador de tráfico de MAC en una regla permite definir criterios de coincidencia para las propiedades de Capa 2 (capa de vínculo de datos) de paquetes como la dirección MAC, el identificador de VLAN y el protocolo de siguiente nivel que consume la carga útil de las tramas.

Tipo de protocolo

El atributo **Tipo de protocolo** del calificador de tráfico de MAC corresponde al campo EtherType en las tramas Ethernet. EtherType representa el tipo de protocolo de siguiente nivel que consumirá la carga útil de la trama.

Puede seleccionar un protocolo en el menú desplegable o escribir el número hexadecimal correspondiente. Por ejemplo, para capturar tráfico del protocolo Link Layer Discovery Protocol (LLDP), escriba `88CC`.

Identificador de VLAN

Puede utilizar el atributo identificador de VLAN del calificador de tráfico de MAC para marcar o filtrar el tráfico de una VLAN particular.

Nota El calificador de identificador de VLAN en un grupo de puertos distribuidos funciona con el etiquetado de invitado virtual (VGT).

Si se etiqueta un flujo con un identificador de VLAN a través del etiquetado de conmutador virtual (VST), no es posible encontrarlo mediante su identificador en una regla en un grupo de puertos distribuidos o un puerto distribuido. La razón es que el conmutador distribuido comprueba las condiciones de la regla, incluido el identificador de VLAN, después de que el conmutador ya ha quitado la etiqueta del tráfico. En este caso, para buscar coincidencias de tráfico por identificador de VLAN, se debe utilizar una regla en un grupo de puertos de vínculo superior o un puerto de vínculo superior.

Dirección de origen

Al utilizar el grupo de atributos Dirección de origen, puede buscar coincidencias con los paquetes según la dirección MAC o la red de origen.

Puede utilizar un operador de comparación para marcar o filtrar los paquetes que tengan o no tengan la dirección o la red de origen especificada.

Puede buscar coincidencias en el origen de tráfico de diferentes formas.

Tabla 8-6. Patrones para el filtrado o el marcado del tráfico por dirección MAC de origen

Parámetros para hacer coincidir la dirección de origen del tráfico	Operador de comparación	Formato de argumento de redes
Dirección MAC	**es** o **no es**	Escriba la dirección MAC para buscar coincidencias. Separe los octetos con dos puntos (:).
Red MAC	**coincide** o **no coincide**	Escriba la dirección más baja de la red y una máscara. Establezca unos en las posiciones de los bits de red y ceros en la porción del host.

Por ejemplo, para una red MAC con el prefijo 05:50:56 y 23 bits de largo, establezca la dirección como **`00:50:56:00:00:00`** y la máscara como **`ff:ff:fe:00:00:00`**.

Dirección de destino

Al utilizar el grupo de atributos Dirección de destino, puede buscar coincidencias con los paquetes según su dirección de destino. Las opciones de dirección MAC de destino tienen el mismo formato que las de la dirección de origen.

Operadores de comparación

Para buscar coincidencias de tráfico de un calificador MAC más adecuadas a sus necesidades, puede utilizar la comparación afirmativa o la negación. Puede utilizar operadores de forma que todos los paquetes, excepto los que tengan atributos determinados, sean abarcados por una regla.

Calificador de tráfico IP

Mediante el uso de un calificador de tráfico IP en una regla, se pueden definir criterios para hacer coincidir el tráfico con las propiedades de la Capa 3 (capa de red), tales como la versión de IP, la dirección IP, el protocolo de siguiente nivel y el puerto.

Protocolo

El atributo **Protocolo** del calificador de tráfico IP representa el protocolo de siguiente nivel que consume la carga útil del paquete. Se puede seleccionar un protocolo en el menú desplegable o se puede introducir su número decimal de acuerdo con RFC 1700.

En los protocolos TCP y UDP, también se puede hacer coincidir el tráfico de acuerdo con los puertos de origen y de destino.

Puerto de origen

Al utilizar el atributo Puerto de origen, se pueden hacer coincidir los paquetes TCP o UDP de acuerdo con el puerto de origen. Tenga en cuenta la dirección del tráfico al hacer coincidir el tráfico con un puerto de origen.

Puerto de destino

Al utilizar el atributo Puerto de destino, se pueden hacer coincidir los paquetes TCP o UDP de acuerdo con el puerto de destino. Tenga en cuenta la dirección del tráfico al hacer coincidir el tráfico con un puerto de destino.

Dirección de origen

Al utilizar el atributo Dirección de origen, se pueden hacer coincidir los paquetes de acuerdo con la dirección de origen o la subred. Tenga en cuenta la dirección del tráfico al hacer coincidir el tráfico con una red o una dirección de origen.

Se puede hacer coincidir el origen del tráfico de varias maneras.

Tabla 8-7. Patrones para filtrar o marcar el tráfico de acuerdo con la dirección IP de origen

Parámetros para hacer coincidir la dirección de origen del tráfico	Operador de comparación	Formato de argumento de redes
Versión IP	**cualquiera**	Seleccione la versión IP en el menú desplegable.
Dirección IP	**es** o **no es**	Escriba la dirección IP que desea hacer coincidir.
Subred IP	**coincide** o **no coincide**	Escriba la dirección más baja de la subred y la longitud en bits del prefijo de subred.

Dirección de destino

Utilice Dirección de destino para hacer coincidir los paquetes de acuerdo con la dirección IP, la subred o la versión IP. La dirección de destino tiene el mismo formato que la de origen.

Operadores de comparación

Para que el tráfico en un calificador de IP se ajuste mejor a ciertas necesidades, se puede utilizar la comparación de afirmación o negación. Es posible determinar que todos los paquetes se ajusten al alcance de una regla, excepto los paquetes con ciertos atributos.

Administrar directivas para varios grupos de puertos en vSphere Distributed Switch

Es posible modificar las directivas de redes para varios grupos de puertos en vSphere Distributed Switch.

Requisitos previos

Cree vSphere Distributed Switch con uno o más grupos de puertos.

Procedimiento

1 En vSphere Web Client, desplácese hasta el conmutador distribuido.

2 En el navegador de objetos, haga clic con el botón derecho en el conmutador distribuido y seleccione **Grupo de puertos distribuidos > Administrar grupos de puertos distribuidos**.

3 En la página Seleccionar directivas de grupo de puertos, active la casilla que está junto a las categorías de directivas que desea modificar y haga clic en **Siguiente**.

Opción	Descripción
Seguridad	Establezca los cambios en la dirección MAC, las transmisiones falsificadas y el modo promiscuo correspondientes a los grupos de puertos seleccionados.
Catalogación de tráfico	Establezca el ancho de banda promedio, el ancho de banda máximo y el tamaño de ráfaga correspondiente al tráfico entrante y saliente en los grupos de puertos seleccionados.

Opción	Descripción
VLAN	Configure la manera en que los grupos de puertos seleccionados se conectan a las VLAN físicas.
Formación de equipos y conmutación por error	Establezca el equilibrio de carga, la detección de la conmutación por error, la notificación del conmutador y el orden de la conmutación por error correspondientes a los grupos de puertos seleccionados.
Asignación de recursos	Establezca la asociación del grupo de recursos de red correspondiente a los grupos de puertos seleccionados. Esta opción está disponible para vSphere Distributed Switch versión 5.0 y posterior.
Supervisión	Habilite o deshabilite NetFlow en los grupos de puertos seleccionados. Esta opción está disponible para vSphere Distributed Switch versión 5.0.0 y posterior.
Filtrado y marcado de tráfico	Configure la directiva para el filtrado (permitir o descartar) y para el marcado de ciertos tipos de tráfico a través de los puertos de los grupos de puertos seleccionados. Esta opción está disponible para vSphere Distributed Switch versión 5.5 y posterior.
Varios	Habilite o deshabilite el bloqueo de puertos en los grupos de puertos seleccionados.

4 En la página Seleccionar grupos de puertos, seleccione los grupos de puertos distribuidos que desea editar y haga clic en **Siguiente**.

5 (opcional) En la página Seguridad, utilice los menús desplegables para editar las excepciones de seguridad y haga clic en **Siguiente**.

Opción	Descripción
Modo promiscuo	■ **Rechazar**. Colocar un adaptador invitado en modo promiscuo no determina qué tramas recibe el adaptador. ■ **Aceptar**. La colocación de un adaptador invitado en modo promiscuo hace que este detecte todos las tramas transmitidas a vSphere Distributed Switch que están permitidas según la directiva de VLAN para el grupo de puertos al que está conectado el adaptador.
Cambios de dirección MAC	■ **Rechazar**. Si se establece en **Rechazar** y el sistema operativo invitado cambia la dirección MAC del adaptador a otra distinta de la que está en el archivo de configuración `.vmx`, se descartarán todas las tramas entrantes. Si el sistema operativo invitado vuelva a cambiar la dirección MAC para que coincida con la dirección MAC del archivo de configuración `.vmx`, se vuelven a pasar las tramas entrantes. ■ **Aceptar**. El cambio de la dirección MAC desde el sistema operativo invitado tiene el efecto deseado, es decir, se reciben las tramas en la nueva dirección MAC.
Transmisiones falsificadas	■ **Rechazar**. Se descartará toda trama saliente con una dirección MAC de origen que sea diferente de la establecida actualmente en el adaptador. ■ **Aceptar**. No se realizará ningún filtrado y se pasarán todas las tramas salientes.

6 (opcional) En la página Catalogación de tráfico, utilice los menús desplegables para habilitar o deshabilitar la catalogación de tráfico de ingreso o de egreso y haga clic en **Siguiente**.

Opción	Descripción
Estado	Si se habilita **Catalogación de tráfico de ingreso** o **Catalogación de tráfico de egreso**, se establecen límites en la cantidad de ancho de banda de redes asignada para cada adaptador de VMkernel o para el adaptador de red virtual asociado a este grupo de puertos. Si se deshabilita esta directiva, los servicios establecen una conexión libre y clara con la red física de forma predeterminada.
Ancho de banda promedio	Establece la cantidad de bits por segundo que se asignan en un puerto, promediada en el tiempo, es decir, la carga promedio permitida.
Ancho de banda máximo	Es la cantidad máxima de bits por segundo que se permite en un puerto cuando este envía o recibe una ráfaga de tráfico. Este número máximo superará el ancho de banda que un puerto utilice cada vez que este utilice las ráfagas adicionales.
Tamaño de ráfaga	Es la cantidad máxima de bytes que se permiten en una ráfaga. Si se establece este parámetro, un puerto podría recibir una ráfaga adicional cuando no utiliza todo el ancho de banda asignado. Cada vez que el puerto necesite más ancho de banda que el especificado en **Ancho de banda**, se le podrá permitir que transmita datos a una velocidad mayor si estuviera disponible una ráfaga adicional. Este parámetro supera la cantidad de bytes que se pueden acumular en la ráfaga adicional y que se pueden transferir a una velocidad mayor.

7 (opcional) En la página VLAN, utilice los menús desplegables para editar la directiva de VLAN y haga clic en **Siguiente**.

Opción	Descripción
Ninguna	No utilice la VLAN.
VLAN	En el campo **Identificador de VLAN**, escriba un número entre 1 y 4094.
enlace troncal de VLAN	Introduzca un **Rango troncal de VLAN**.
VLAN privada	Seleccione una VLAN privada disponible que desee utilizar.

8 (opcional) En la página Formación de equipos y conmutación por error, utilice los menús desplegables para editar la configuración y haga clic en **Siguiente**.

Opción	Descripción
Equilibrio de carga	La formación de equipos basada en IP requiere que el conmutador físico se configure con el EtherChannel. Para todas las demás opciones, el EtherChannel se debe deshabilitar. Seleccione la manera de elegir un vínculo superior. ■ **Enrutar según el puerto virtual de origen**. Elija un vínculo superior basado en el puerto virtual por donde el tráfico entró al conmutador distribuido. ■ **Enrutar según el hash de IP**. Elija un vínculo superior basado en un hash de las direcciones IP de origen y de destino de cada paquete. Para los paquetes que no utilizan IP, lo que se encuentre en estos desplazamientos se utiliza para calcular el hash. ■ **Enrutar según el hash de MAC de origen**. Elija un vínculo superior basado en un hash de la Ethernet de origen. ■ **Enrutar según la carga de la NIC física**. Elija un vínculo superior basado en las cargas actuales de las NIC físicas. ■ **Utilizar orden explícito de conmutación por error**. Utilice siempre el vínculo superior más elevado de la lista de adaptadores activos, el cual cumple los criterios de detección de conmutación por error.
Detección de errores de red	Seleccione el método que desea utilizar para la detección de conmutación por error. ■ **Solo estado de vínculo**: se basa solamente en el estado del vínculo que proporciona el adaptador de red. Esta opción detecta errores, como cables extraídos y errores de alimentación de conmutadores físicos, pero no errores de configuración, como puertos de conmutadores físicos bloqueados por árboles de expansión o configurados hacia la VLAN incorrecta, o cables extraídos en el otro extremo de un conmutador físico. ■ **Sondeo de señal**. Envía y escucha sondas de señal en todas las NIC del equipo, y utiliza esta información, además del estado del vínculo, para determinar el error en el vínculo. No utilice sondeo de señal con equilibrio de carga de hash de IP.
Notificar a conmutadores	Seleccione **Sí** o **No** para notificar a los conmutadores en caso de una conmutación por error. No utilice esta opción cuando las máquinas virtuales que utilizan el grupo de puertos estén utilizando el equilibrio de carga de red de Microsoft en modo de unidifusión. Si selecciona **Sí**, cada vez que una NIC virtual esté conectada al conmutador distribuido o cada vez que el tráfico de la NIC virtual se enrute a través de una NIC física diferente en el equipo debido a un evento de conmutación por error, se envía una notificación por la red para actualizar las tablas de búsqueda en los conmutadores físicos. Utilice este proceso para obtener la menor latencia de migraciones y ocurrencias de conmutación por error con vMotion.

Opción	Descripción
Conmutación por recuperación	Seleccione **Sí** o **No** para habilitar o deshabilitar la conmutación por recuperación. Esta opción determina de qué forma un adaptador físico vuelve a activarse después de recuperarse de un error. ■ **Sí** (valor predeterminado). El adaptador vuelve a servicio activo inmediatamente después de la recuperación, desplazando a cualquier adaptador en espera que hubiera ocupado su ranura. ■ **No**. Un adaptador con errores se deja inactivo incluso después de la recuperación hasta que otro adaptador actualmente activo presente errores y requiera su sustitución.
Orden de conmutación por error	Seleccione la manera de distribuir la carga de trabajo entre los vínculos superiores. Para utilizar algunos vínculos superiores, pero reservar otros en caso de que los vínculos superiores en uso presenten errores, establezca esta condición moviéndolos a diferentes grupos. ■ **Vínculos superiores activos**. Siga utilizando el vínculo superior si la conectividad del adaptador de red está activa y en funcionamiento. ■ **Vínculos superiores en espera**. Utilice este vínculo superior si la conectividad de uno de los adaptadores activos está desactivada. Cuando se utilice el equilibrio de carga de hash de IP, no configure vínculos superiores en espera. ■ **Vínculos superiores sin utilizar**. No utilice este vínculo superior.

9 (opcional) En la página Asignación de recursos, utilice el menú desplegable **Grupo de recursos de red** para agregar o quitar asignaciones de recursos y, a continuación, haga clic en **Siguiente**.

10 (opcional) En la página Supervisión, utilice el menú desplegable para habilitar o deshabilitar NetFlow y haga clic en **Siguiente**.

Opción	Descripción
Deshabilitado	NetFlow está deshabilitado en el grupo de puertos distribuidos.
Habilitado	NetFlow está habilitado en el grupo de puertos distribuidos. Puede configurar las opciones de NetFlow en el nivel de vSphere Distributed Switch.

11 (opcional) En la página Marcado y filtrado de tráfico, habilite o deshabilite la señalización y el filtrado de tráfico en el menú desplegable **Estado**, configure las reglas de tráfico para el filtrado o la señalización de los flujos de datos específicos y haga clic en **Siguiente**.

Puede establecer los siguientes atributos de una regla para determinar el tráfico de destino y la acción que se llevará a cabo en él:

Opción	Descripción
Nombre	Nombre de la regla
Acción	■ **Permitir**. Concede acceso al tráfico de un determinado tipo. ■ **Descartar**. Niega acceso al tráfico de un determinado tipo. ■ **Etiquetar.** Clasifica el tráfico en términos de la calidad de servicio (QoS) mediante la inserción o el reetiquetado del tráfico con CoS y una etiqueta DSCP.
Dirección del tráfico	Establezca si la regla es para el tráfico entrante o saliente, o para ambos. La dirección también influye en la manera en que se va a identificar el origen y el destino del tráfico.
Calificador de tráfico del sistema	Indica que la regla examina el tráfico del sistema y establece el tipo de protocolo de infraestructura al que se aplicará la regla. Por ejemplo, marca con una etiqueta de prioridad el tráfico para la administración desde vCenter Server.

Opción	Descripción
Calificador de MAC	Califica el tráfico correspondiente a la regla por el encabezado de Capa 2. ■ **Tipo de protocolo**. Establezca el protocolo de siguiente nivel (IPv4, IPv6, etc.) que consume la carga útil. Este atributo corresponde al campo EtherType en tramas Ethernet. Puede seleccionar un protocolo en el menú desplegable o escribir su número hexadecimal. Por ejemplo, para localizar el tráfico correspondiente al protocolo Link Layer Discovery Protocol (LLDP), escriba **`88CC`**. ■ **Identificador de VLAN**. Localice el tráfico por VLAN. El calificador de identificador de VLAN en un grupo de puertos distribuidos funciona con el etiquetado de invitado virtual (VGT). Si tiene un flujo etiquetado con un identificador de VLAN a través del etiquetado de conmutador virtual (VST), no puede localizar el flujo de este identificador en una regla de grupo de puertos distribuidos. La razón es que el conmutador distribuido comprueba las condiciones de la regla, incluido el identificador de VLAN, después de que el conmutador ya ha quitado la etiqueta del tráfico. Para que el tráfico coincida correctamente con un identificador de VLAN, utilice una regla para un grupo de puertos de vínculo superior o un puerto de vínculo superior. ■ **Dirección de origen**. Establezca una única dirección MAC o una red MAC para que coincida con los paquetes por dirección de origen. Para una red MAC, introduzca la dirección más baja en la red y una máscara comodín. La máscara contiene ceros en las posiciones de los bits de red y unos en la parte del host. Por ejemplo, para una red MAC con el prefijo 05:50:56 que tiene 23 bits de longitud, establezca la dirección como **`00:50:56:00:00:00`** y la máscara como **`00:00:01:ff:ff:ff`**. ■ **Dirección de destino**. Establezca una única dirección MAC o una red MAC para que coincida con los paquetes por dirección de destino. La dirección de destino MAC admite el mismo formato que la dirección de origen.
Calificador de IP	Califica el tráfico correspondiente a la regla por el encabezado de Capa 3. ■ **Protocolo**. Establezca el protocolo de siguiente nivel (TCP, UDP, etc.) que consume la carga útil. Puede seleccionar un protocolo en el menú desplegable o puede escribir su número decimal de acuerdo con *RFC 1700, Assigned Numbers*. Para TCP y UDP, también se puede establecer el puerto de destino y de origen. ■ **Puerto de origen**. Hace coincidir los paquetes TCP o UDP con un puerto de origen. Cuando determine el puerto de origen con el que deben coincidir los paquetes, tenga en cuenta la dirección del tráfico que está dentro del alcance de la regla. ■ **Puerto de destino**. Hace coincidir los paquetes TCP o UDP por el puerto de origen. Cuando determine el puerto de destino con el que deben coincidir los paquetes, tenga en cuenta la dirección del tráfico que está dentro del alcance de la regla.

Opción	Descripción
	■ **Dirección de origen**. Establezca la versión IP, una única dirección IP o una subred para que coincidan con los paquetes por la dirección de origen. Para una subred, introduzca la dirección más baja y la longitud del prefijo en bits. ■ **Dirección de destino**. Establezca la versión IP, una única dirección IP o una subred para que coincidan con los paquetes por la dirección de origen. La dirección IP de destino admite el mismo formato que la dirección de origen.

12 (opcional) En la página Varios, seleccione **Sí** o **No** en el menú desplegable y haga clic en **Siguiente**.

Seleccione **Sí** para apagar todos los puertos en el grupo de puertos. Este apagado podría interrumpir las operaciones normales de la red de los hosts o de las máquinas virtuales que utilicen los puertos.

13 Revise la información de la página Listo para finalizar y haga clic en **Finalizar**.

Utilice el botón **Atrás** para cambiar cualquier configuración.

Directivas de bloqueo de puertos

Las directivas de bloqueo de puertos permiten bloquear selectivamente el envío o la recepción de datos en los puertos.

Editar la directiva de bloqueo de puertos para un grupo de puertos distribuidos

Puede bloquear todos los puertos de un grupo de puertos distribuidos.

Bloquear los puertos de un grupo de puertos distribuidos puede interrumpir las operaciones de red normales de los hosts o las máquinas virtuales que usan los puertos.

Procedimiento

1 En vSphere Web Client, desplácese hasta el conmutador distribuido.

2 En el navegador de objetos, haga clic con el botón derecho en el conmutador distribuido y seleccione **Grupo de puertos distribuidos > Administrar grupos de puertos distribuidos**.

3 Active la casilla **Varios** y haga clic en **Siguiente**.

4 Seleccione uno o más grupos de puertos distribuidos que se configurarán y haga clic en **Siguiente**.

5 Habilite o deshabilite el bloqueo de puertos en el menú desplegable **Bloquear todos los puertos** y haga clic en **Siguiente**.

6 Repase la configuración y haga clic en **Finalizar**.

Editar la directiva de bloqueo para un puerto distribuido o un puerto de vínculo superior

Puede bloquear un puerto distribuido individual o un puerto de vínculo superior.

Bloquear el flujo a través de un puerto puede interrumpir las operaciones de red normales en el host o la máquina virtual que usa el puerto.

Requisitos previos

Habilite la anulación en el nivel de los puertos. Consulte Configurar las directivas de red de anulación en los puertos

Procedimiento

1 Desplácese hasta un conmutador distribuido y después hasta un puerto distribuido o un puerto de vínculo superior.

- Para desplazarse hasta los puertos distribuidos del conmutador, haga clic en **Redes > Grupos de puertos distribuidos**, haga doble clic en un grupo de puertos distribuidos de la lista y, a continuación, haga clic en la pestaña **Puertos**.
- Para desplazarse hasta los puertos de vínculo superior de un grupo de puertos de vínculo superior, haga clic en **Redes > Grupos de puertos de vínculo superior**, haga doble clic en un grupo de puertos de vínculo superior de la lista y, a continuación, haga clic en la pestaña **Puertos**.

2 Seleccione un puerto de la lista.

3 Haga clic en **Editar configuración de puertos distribuidos**.

4 En la sección **Varios**, active la casilla **Anular** y, en el menú desplegable, habilite o deshabilite el bloqueo de puertos.

5 Haga clic en **Aceptar**.

Aislar el tráfico de red mediante VLAN

9

Las VLAN permiten segmentar una red en varios dominios de difusión lógicos en la Capa 2 de la pila del protocolo de red.

Este capítulo incluye los siguientes temas:

Configuración de VLAN

Las LAN virtuales (VLAN) permiten que se aísle aún más un único segmento LAN físico para que los grupos de puertos se aíslen los unos de los otros como si estuvieran en segmentos físicamente diferentes.

Beneficios de usar VLAN en vSphere

La configuración de VLAN en un entorno de vSphere aporta ciertos beneficios.

- Integra los hosts ESXi en una topología de VLAN previa.
- Aísla y protege el tráfico de red.
- Reduce la congestión del tráfico de red.

Vea el vídeo sobre los beneficios y los principios clave para incorporar VLAN en un entorno de vSphere.

Usar VLAN en un entorno de vSphere
(https://vmwaretv.vmware.com/media/t/1_hff29dl8)

Modos de etiquetado de VLAN

vSphere admite tres modos de etiquetado de VLAN en ESXi: etiquetado de conmutador externo (EST), etiquetado de conmutador virtual (VST) y etiquetado de invitado virtual (VGT).

Modo de etiquetado	Identificador de VLAN en grupos de puertos de conmutador	Descripción
EST	0	El conmutador físico ejecuta el etiquetado de VLAN. Los adaptadores de red de host se conectan para tener acceso a los puertos del conmutador físico.
VST	Entre 1 y 4.094	El conmutador virtual ejecuta el etiquetado de VLAN antes de que los paquetes salgan del host. Los adaptadores de red de host se conectan a puertos troncales del conmutador físico.
VGT	■ 4.095 para el conmutador estándar ■ Rango de VLAN y VLAN individuales para el conmutador distribuido	La máquina virtual ejecuta el etiquetado de VLAN. El conmutador virtual conserva las etiquetas de VLAN cuando reenvía los paquetes entre la pila de redes de máquina virtual y el conmutador externo. Los adaptadores de red de host se conectan a puertos troncales del conmutador físico. vSphere Distributed Switch admite la modificación de VGT. Por motivos de seguridad, puede configurar un conmutador distribuido para transmitir exclusivamente los paquetes que pertenecen a VLAN específicas. **Nota** Para VGT, se necesita un controlador de enlace troncal de VLAN 802.1Q instalado en el sistema operativo invitado de la máquina virtual.

Vea el vídeo que explica los modos de etiquetado de VLAN en conmutadores virtuales.

Modos de etiquetado de VLAN en vSphere
(https://vmwaretv.vmware.com/media/t/1_3bluh3s4)

VLAN privadas

Las VLAN privadas permiten resolver las limitaciones de identificador de VLAN al agregar una segmentación adicional del dominio de difusión lógico en varios subdominios de difusión más reducidos.

Una VLAN privada se identifica con el identificador de VLAN principal. Un identificador de VLAN principal puede tener varios identificadores de VLAN secundarios asociados. Las VLAN principales son **Promiscuas** para que los puertos de una VLAN privada puedan comunicarse con puertos configurados como la VLAN principal. Los puertos en una VLAN secundaria pueden ser **Aislados** y comunicarse solo con puertos promiscuos o **Comunitarios** y comunicarse tanto con puertos promiscuos como con otros en la misma VLAN secundaria.

Para utilizar VLAN privadas entre un host y el resto de la red física, el conmutador físico conectado al host necesita ser compatible con VLAN privada y estar configurado con los identificadores de VLAN que utiliza ESXi para la funcionalidad de VLAN privada. En el caso de los conmutadores físicos que utilizan aprendizaje basado en identificador de MAC+VLAN, todos los identificadores de VLAN privados correspondientes primero deben introducirse a la base de datos VLAN del conmutador.

Crear una VLAN privada

Cree las VLAN privadas que necesite en vSphere Distributed Switch para poder asignar puertos distribuidos que formen parte de una VLAN privada.

Procedimiento

1 En vSphere Web Client, desplácese hasta el conmutador distribuido.

2 En la pestaña **Configurar**, expanda **Configuración** y seleccione **VLAN privada**.

3 Haga clic en **Editar**.

4 Para agregar una VLAN principal, en Identificador de VLAN principal haga clic en **Agregar** y escriba el identificador de una VLAN principal.

5 Haga clic en el **signo más (+)** junto al identificador de la VLAN principal para agregarla a la lista.

   La VLAN privada principal también aparece en Identificador de VLAN privada secundaria.

6 Para agregar una VLAN secundaria, en el panel derecho, haga clic en **Agregar** y escriba el identificador de la VLAN.

7 Haga clic en el **signo más (+)** junto al identificador de la VLAN secundaria para agregarla a la lista.

8 En el menú desplegable de la columna **Tipo de VLAN secundaria**, seleccione **Aislada** o **Comunitaria**.

9 Haga clic en **Aceptar**.

Pasos siguientes

Configure un grupo de puertos distribuidos o un puerto para asociar el tráfico con la VLAN privada. Consulte Configurar etiquetado de VLAN en un grupo de puertos distribuidos o un puerto distribuido.

Quitar una VLAN privada principal

Quite las VLAN principales sin usar de la configuración de vSphere Distributed Switch.

Al quitar una VLAN privada principal, también se quitan las VLAN privadas secundarias asociadas.

Requisitos previos

Compruebe que no haya grupos de puertos configurados para usar la VLAN principal y sus VLAN secundarias asociadas.

Procedimiento

1 En vSphere Web Client, desplácese hasta el conmutador distribuido.

2 En la pestaña **Configurar**, expanda **Configuración** y seleccione **VLAN privada**.

3 Haga clic en **Editar**.

4 Seleccione la VLAN privada principal que desea quitar.

5 Haga clic en **Quitar** en la lista identificador de VLAN principal.

6 Haga clic en **Aceptar** para confirmar que desea quitar la VLAN principal.

7 Haga clic en **Aceptar**.

Quitar una VLAN privada secundaria

Quite las VLAN privadas secundarias sin usar de la configuración de vSphere Distributed Switch.

Requisitos previos

Compruebe que no haya grupos de puertos configurados para usar la VLAN secundaria.

Procedimiento

1 En vSphere Web Client, desplácese hasta el conmutador distribuido.

2 En la pestaña **Configurar**, expanda **Configuración** y seleccione **VLAN privada**.

3 Haga clic en **Editar**.

4 Seleccione una VLAN privada principal.

  Las VLAN privadas secundarias asociadas se muestran a la derecha.

5 Seleccione la VLAN privada secundaria que desea quitar.

6 En la lista de identificador de VLAN secundarias, haga clic en **Quitar** y, a continuación, en **Aceptar**.

Administrar los recursos de la red 10

vSphere ofrece varios métodos diferentes para ayudar a administrar los recursos de la red.

Este capítulo incluye los siguientes temas:

DirectPath I/O

DirectPath I/O permite el acceso de las máquinas virtuales a las funciones PCI físicas en plataformas con una unidad de administración de memoria de E/S.

Las siguientes características no están disponibles para máquinas virtuales configuradas con DirectPath:

- Agregado y eliminación en caliente de dispositivos virtuales
- Suspensión y reanudación
- Registro y reproducción
- Tolerancia a errores
- Alta disponibilidad
- DRS (disponibilidad limitada. La máquina virtual puede ser parte de un clúster, pero no puede migrar entre los hosts)
- Instantáneas

Las siguientes características solo están disponibles para máquinas virtuales configuradas con DirectPath I/O en sistemas informáticos unificados (UCS) de Cisco mediante conmutadores distribuidos Cisco Virtual Machine Fabric Extender (VM-FEX).

- vMotion
- Agregado y eliminación en caliente de dispositivos virtuales
- Suspensión y reanudación
- Alta disponibilidad
- DRS
- Instantáneas

Consulte la documentación de Cisco VM-FEX para obtener detalles sobre los conmutadores compatibles e información sobre la configuración de conmutadores.

- Habilitar el acceso directo de un dispositivo de red en un host

  Los dispositivos de acceso directo permiten utilizar los recursos con eficacia y mejorar el rendimiento del entorno. Puede habilitar el acceso directo de DirectPath I/O para un dispositivo de red en un host.

- Configurar un dispositivo PCI en una máquina virtual

  Los dispositivos de acceso directo permiten usar los recursos con mayor eficacia y mejorar el rendimiento del entorno. Puede configurar un dispositivo PCI de acceso directo en una máquina virtual de vSphere Web Client.

- Habilitar DirectPath I/O con vMotion en una máquina virtual

  Puede habilitar DirectPath I/O con vMotion para las máquinas virtuales de un centro de datos en un sistema Cisco UCS. El sistema debe tener al menos un conmutador distribuido de Cisco UCS Virtual Machine Fabric Extender (VM-FEX) compatible.

Habilitar el acceso directo de un dispositivo de red en un host

Los dispositivos de acceso directo permiten utilizar los recursos con eficacia y mejorar el rendimiento del entorno. Puede habilitar el acceso directo de DirectPath I/O para un dispositivo de red en un host.

Precaución Si el host ESXi está configurado para arrancar desde un dispositivo USB o una tarjeta SD conectada a un canal USB, asegúrese de que el acceso directo de DirectPath I/O no esté habilitado para la controladora USB. El paso a través de una controladora USB en un host ESXi que arranca desde un dispositivo USB o una tarjeta SD puede dejar el host en un estado en que no se conserve la configuración.

Procedimiento

1. Desplácese hasta un host en el navegador de vSphere Web Client.
2. En la pestaña **Configurar**, expanda **Hardware** y haga clic en **Dispositivos PCI**.

3 Para habilitar el acceso directo de DirectPath I/O para un dispositivo de red PCI en el host, haga clic en **Editar**.

   Aparece una lista de dispositivos de acceso directo disponibles.

Icono	Descripción
Icono verde	El dispositivo está activo y puede ser habilitado.
Icono naranja	Cambió el estado del dispositivo, es necesario reiniciar el host para poder utilizarlo.

4 Seleccione el dispositivo de red que se utilizará para el acceso directo y haga clic en **Aceptar**.

   El dispositivo PCI seleccionado aparece en la tabla. En la parte inferior de la pantalla se muestra información sobre el dispositivo.

5 Reinicie el host para que el dispositivo de red PCI esté disponible para utilizar.

Configurar un dispositivo PCI en una máquina virtual

Los dispositivos de acceso directo permiten usar los recursos con mayor eficacia y mejorar el rendimiento del entorno. Puede configurar un dispositivo PCI de acceso directo en una máquina virtual de vSphere Web Client.

Si usa dispositivos de acceso directo con un kernel Linux 2.6.20, o versiones anteriores, no use los modos MSI y MSI-X, ya que pueden reducir significativamente el rendimiento.

Requisitos previos

Compruebe que haya un dispositivo de red de acceso directo configurado en el host de la máquina virtual. Consulte Habilitar el acceso directo de un dispositivo de red en un host.

Procedimiento

1 Ubique la máquina virtual en vSphere Web Client.

   a Seleccione un centro de datos, una carpeta, un clúster, un grupo de recursos o un host y haga clic en la pestaña **Máquinas virtuales**.

   b Haga clic en **Máquinas virtuales** y haga doble clic en la máquina virtual en la lista.

2 Apague la máquina virtual.

3 En la pestaña **Configurar** de la máquina virtual, expanda **Configuración** y seleccione **Hardware de máquina virtual**.

4 Haga clic en **Editar** y seleccione la pestaña **Hardware virtual** en el cuadro de diálogo que se muestra en la configuración.

5 Expanda la sección **Memoria** y establezca la opción **Límite** en **Ilimitado**.

6 En el menú desplegable **Nuevo dispositivo**, seleccione **Dispositivo PCI** y haga clic en **Agregar**.

7 En el menú desplegable **Nuevo dispositivo PCI**, seleccione el dispositivo de acceso directo que desea usar y haga clic en **Aceptar**.

8 Encienda la máquina virtual.

Resultados

Cuando se agrega un dispositivo con DirectPath I/O a una máquina virtual, se establece la reserva de memoria con el tamaño de memoria de la máquina virtual.

Habilitar DirectPath I/O con vMotion en una máquina virtual

Puede habilitar DirectPath I/O con vMotion para las máquinas virtuales de un centro de datos en un sistema Cisco UCS. El sistema debe tener al menos un conmutador distribuido de Cisco UCS Virtual Machine Fabric Extender (VM-FEX) compatible.

Requisitos previos

Habilite una E/S de red de alto rendimiento en al menos un perfil de puerto Cisco UCS de un conmutador distribuido Cisco VM-FEX compatible. Para obtener más información sobre los conmutadores compatibles y su configuración, consulte la documentación disponible en el sitio web de http://www.cisco.com/go/unifiedcomputing/b-series-doc.

Procedimiento

1 Ubique la máquina virtual en vSphere Web Client.

   a Seleccione un centro de datos, una carpeta, un clúster, un grupo de recursos o un host y haga clic en la pestaña **Máquinas virtuales**.

   b Haga clic en **Máquinas virtuales** y haga doble clic en la máquina virtual en la lista.

2 Apague la máquina virtual.

3 En la pestaña **Configurar** de la máquina virtual, expanda **Configuración** y seleccione **Hardware de máquina virtual**.

4 Haga clic en **Editar** y seleccione la pestaña **Hardware virtual** en el cuadro de diálogo que se muestra en la configuración.

5 Expanda la sección **Memoria** y establezca la opción **Límite** en **Ilimitado**.

6 Expanda la sección **Adaptador de red** para configurar un dispositivo de acceso directo.

7 Junto a DirectPath I/O, haga clic en **Habilitar**.

8 En el menú desplegable de red, seleccione un perfil de puerto con alto rendimiento habilitado y haga clic en **Aceptar**.

9 Encienda la máquina virtual.

Virtualización de E/S de raíz única (SR-IOV)

vSphere 5.1 y versiones posteriores admiten la virtualización de E/S de raíz única (SR-IOV). Se puede utilizar la SR-IOV para conectar en red máquinas virtuales sujetas a latencia o que requieren más recursos de CPU.

Descripción general de SR-IOV

SR-IOV es una especificación que permite que un único dispositivo físico de interconexión de componentes periféricos express (PCIe) de un solo puerto raíz aparezca como varios dispositivos físicos distintos ante el hipervisor o el sistema operativo invitado.

SR-IOV utiliza funciones físicas (PF) y funciones virtuales (VF) para administrar funciones globales de los dispositivos de SR-IOV. Las PF son funciones de PCIe completas que pueden configurar y administrar la funcionalidad de SR-IOV. Con las PF, se pueden configurar o controlar dispositivos PCIe, y la PF tiene capacidad total para poner y sacar datos en el dispositivo. Las VF son funciones de PCIe ligeras que admiten el flujo de datos, pero que tienen un conjunto restringido de recursos de configuración.

La cantidad de funciones virtuales que se proporciona al hipervisor o al sistema operativo invitado depende del dispositivo. Los dispositivos PCIe habilitados para SR-IOV requieren la compatibilidad correspondiente con el hardware y el BIOS, como también compatibilidad de SR-IOV en la instancia de hipervisor o el controlador del sistema operativo invitado. Consulte Compatibilidad con SR-IOV.

Usar SR-IOV en vSphere

En vSphere, una máquina virtual puede utilizar una función virtual de SR-IOV para las redes. La máquina virtual y el adaptador físico intercambian datos directamente sin utilizar el VMkernel como instancia intermediaria. La omisión del VMkernel en las redes reduce la latencia y mejora la eficiencia de la CPU.

En vSphere 5.5 y versiones posteriores, si bien un conmutador virtual (conmutador estándar o distribuido) no controla el tráfico de red de una máquina virtual habilitada para SR-IOV conectada al conmutador, es posible controlar las funciones virtuales asignadas mediante las directivas de configuración de conmutadores en el nivel de puerto o grupo de puertos.

Compatibilidad con SR-IOV

vSphere 5.1 y las versiones posteriores admiten SR-IOV exclusivamente en entornos con una configuración específica. Algunas características de vSphere no funcionan cuando se habilita SR-IOV.

Tipos de configuración compatibles

Para usar SR-IOV en vSphere 6.0, el entorno debe cumplir con varios requisitos de configuración.

Tabla 10-1. Tipos de configuración compatibles para usar SR-IOV

Componente	Requisitos
vSphere	■ Los hosts con procesadores Intel requieren ESXi 5.1 o versiones posteriores. ■ Los hosts con procesadores AMD son compatibles con SR-IOV en ESXi 5.5 o versiones posteriores.
Host físico	■ Debe ser compatible con la versión de ESXi. ■ Debe tener un procesador Intel si se ejecuta ESXi 5.1, o un procesador Intel o AMD si se ejecuta ESXi 5.5 o versiones posteriores. ■ Debe admitir la unidad de administración de memoria de E/S (IOMMU) y tener la unidad IOMMU habilitada en el BIOS. ■ Debe admitir SR-IOV y tener SR-IOV habilitado en el BIOS. Póngase en contacto con el proveedor del servidor para determinar si el host admite SR-IOV.
NIC física	■ Debe ser compatible con la versión de ESXi. ■ Debe ser compatible con el host y SR-IOV según la documentación técnica suministrada por el proveedor del servidor. ■ Debe tener SR-IOV habilitado en el firmware. ■ Debe utilizar interrupciones MSI-X.
Controlador de PF en ESXi para la NIC física	■ Debe estar certificado por VMware. ■ Debe estar instalado en el host ESXi. La versión de ESXi incluye un controlador predeterminado para algunas NIC, pero es necesario descargar e instalar manualmente el controlador para otras NIC.
Sistema operativo invitado	Debe ser compatible con la NIC en la versión de ESXi instalada, según se indica en la documentación técnica del proveedor de la NIC.
Controlador de VF en el sistema operativo invitado	■ Debe ser compatible con la NIC. ■ Debe ser compatible con la versión de sistema operativo invitado, según se indica en la documentación técnica del proveedor de la NIC. ■ Debe tener un certificado WLK o WHCK de Microsoft para máquinas virtuales de Windows. ■ Debe estar instalado en el sistema operativo. La versión de sistema operativo incluye un controlador predeterminado para ciertas NIC, pero otras requieren descargar el controlador de una ubicación suministrada por el proveedor de la NIC o del host e instalarlo.

Para comprobar que los hosts físicos y las NIC sean compatibles con las versiones de ESXi, consulte la *Guía de compatibilidad de VMware*.

Disponibilidad de características

Las siguientes características no están disponibles en las máquinas virtuales configuradas con SR-IOV:

- vSphere vMotion
- Storage vMotion
- vShield
- NetFlow
- VXLAN Virtual Wire
- vSphere High Availability
- vSphere Fault Tolerance
- vSphere DRS
- vSphere DPM
- Suspensión y reanudación de la máquina virtual
- Instantáneas de la máquina virtual
- VLAN basada en MAC para funciones virtuales de acceso directo
- Adición y extracción en caliente de dispositivos virtuales, memoria y vCPU
- Participación en un entorno de clúster
- Estadísticas de red para una NIC de máquina virtual donde se use SR-IOV de acceso directo

---

Nota Si se intenta habilitar o configurar las características no compatibles con SR-IOV en vSphere Web Client, se observará un comportamiento inesperado en el entorno.

NIC compatibles

Todas las NIC deben tener controladores y firmware compatibles con SR-IOV. En algunas NIC, SR-IOV debe estar habilitado en el firmware. Para saber qué NIC son compatibles con las máquinas virtuales configuradas con SR-IOV, consulte la Guía de compatibilidad de VMware.

Actualizar desde vSphere 5.0 y versiones anteriores

Si se actualiza desde vSphere 5.0 o una versión anterior hacia vSphere 5.5 o una versión posterior, SR-IOV recién se admite cuando se actualizan los controladores de NIC para la versión de vSphere. El firmware y los controladores que admiten SR-IOV deben habilitarse en las NIC para poder usar la funcionalidad SR-IOV.

Actualizar desde vSphere 5.1

Si bien SR-IOV es compatible con los hosts ESXi 5.1 que cumplen con los requisitos, no es posible configurar SR-IOV en ellos desde vSphere Web Client. Use el parámetro `max_vfs` del módulo de controladores de NIC para habilitar SR-IOV en estos hosts. Consulte Habilitar SR-IOV mediante perfiles de host o un comando ESXCLI.

Tampoco se puede asignar un adaptador de acceso directo de SR-IOV a una máquina virtual en este host. El adaptador está disponible para las máquinas virtuales compatibles con ESXi 5.5 y versiones posteriores. Si bien la versión vCenter Server 5.5 puede administrar un host ESXi 5.1, la configuración es igual a la de la versión 5.1. Debe agregar un dispositivo PCI al hardware de la máquina virtual y seleccionar manualmente una VF para el dispositivo.

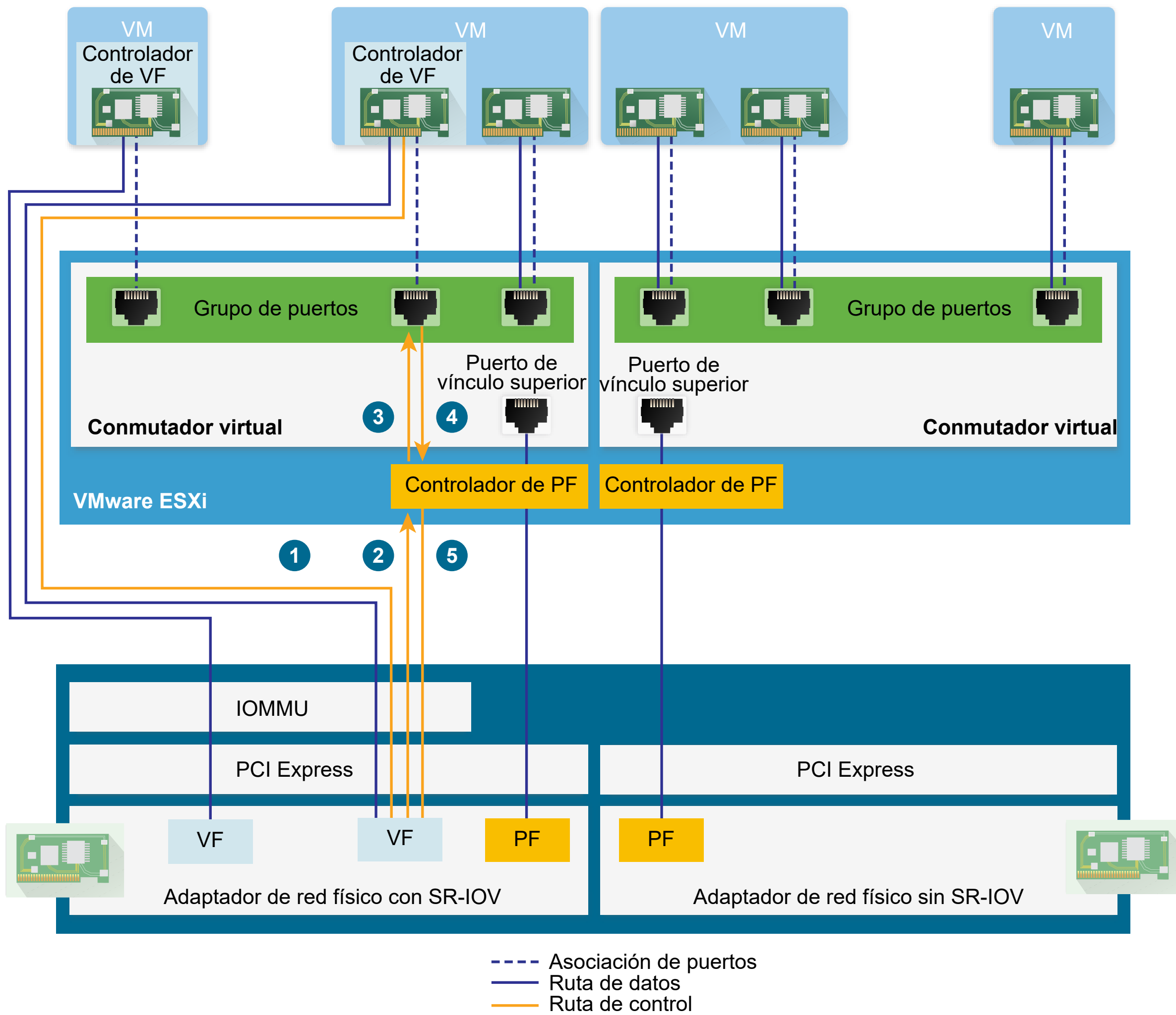
Interacción y arquitectura del componente SR-IOV

La compatibilidad de SR-IOV con vSphere depende de la interacción entre las funciones virtuales (VF) y la función física (PF) del puerto de NIC para lograr un mejor rendimiento, y de la interacción entre el controlador de la PF y el conmutador del host para el control de tráfico.

En un host donde se ejecuta el tráfico de máquina virtual sobre los adaptadores físicos SR-IOV, los adaptadores de la máquina virtual se comunican directamente con las funciones virtuales para transferir datos. No obstante, la capacidad para configurar redes depende de las directivas activas para el puerto donde se alojan las máquinas virtuales.

En un host ESXi sin SR-IOV, el conmutador virtual envía el tráfico de red externo a través de sus puertos en el host desde el adaptador físico del grupo de puertos relevante o hacia ese adaptador. El conmutador virtual también aplica las directivas de red a los paquetes administrados.

Figura 10-1. Rutas de datos y configuración para la compatibilidad de SR-IOV con vSphere



Ruta de datos en SR-IOV

Una vez que se asigna el adaptador de red de máquina virtual a una función virtual, el controlador de VF del sistema operativo invitado usa la tecnología de unidad de administración de memoria de E/S (IOMMU) para tener acceso a la función virtual que debe recibir o enviar los datos a través de la red. El VMkernel, es decir, el conmutador virtual específico, no procesa el flujo de datos, lo cual reduce la latencia general de las cargas de trabajo con SR-IOV.

Ruta de configuración en SR-IOV

Si el sistema operativo invitado intenta cambiar la configuración de un adaptador de la máquina virtual asignado a una VF, el cambio se aplica si así lo permite la directiva del puerto asociado con el adaptador de la máquina virtual.

El flujo de trabajo de configuración implica las siguientes operaciones:

1 El sistema operativo invitado solicita un cambio de configuración en la VF.

2 La VF reenvía la solicitud a la PF a través de un mecanismo de buzón de correo.

3 El controlador de PF comprueba la solicitud de configuración con el conmutador virtual (conmutador estándar o conmutador proxy del host de un conmutador distribuido).

4 El conmutador virtual comprueba la solicitud de configuración con la directiva del puerto al cual está asociado el adaptador de la máquina virtual con VF.

5 El controlador de PF configura la VF si la nueva configuración cumple con la directiva de puerto del adaptador de la máquina virtual.

   Por ejemplo, si el controlador de VF intenta modificar la dirección MAC, la dirección se conserva si el cambio de dirección MAC está prohibido por la directiva de seguridad para el puerto o el grupo de puertos. El sistema operativo invitado puede indicar que el cambio se efectuó correctamente, pero el registro muestra un mensaje donde se indica que la operación no se pudo realizar. Por lo tanto, el sistema operativo invitado y el dispositivo virtual tienen direcciones MAC diferentes. La interfaz de red del sistema operativo invitado posiblemente no pueda obtener una dirección IP y comunicarse. En este caso, es necesario restablecer la interfaz en el sistema operativo invitado para obtener la dirección MAC actualizada del dispositivo virtual y recibir una dirección IP.

Interacción entre la función virtual y vSphere

Las funciones virtuales (VF) son funciones de PCIe ligeras que contienen todos los recursos necesarios para el intercambio de datos, pero tienen un conjunto reducido de recursos de configuración. La interacción entre vSphere y las VF es limitada.

- La NIC física debe utilizar interrupciones MSI-X.
- Las VF no implementan el control de tasa en vSphere. Cada VF tiene el potencial de usar todo el ancho de banda de un vínculo físico.
- Cuando se configura un dispositivo de VF como dispositivo de acceso directo en una máquina virtual, no se admiten las funciones de espera ni de hibernación de la máquina virtual.
- La cantidad máxima de VF que se pueden crear y la cantidad máxima de VF que se pueden usar para el acceso directo son diferentes. La cantidad máxima de instancias de VF que se pueden ejecutar depende de la capacidad de la NIC y de la configuración de hardware del host. Sin embargo, como la cantidad de vectores de interrupción disponibles para los dispositivos de acceso directo es limitada, solamente es posible usar una cantidad limitada de las instancias de VF en un host ESXi.

  La cantidad total de vectores de interrupción en cada host ESXi puede llegar a 4.096 si se cuenta con 32 CPU.. Cuando el host arranca, los dispositivos en el host, como controladoras de almacenamiento, adaptadores de red físicos y controladoras USB, consumen una subred de 4.096 vectores. Si estos dispositivos requieren más de 1.024 vectores, se reduce la cantidad máxima de VF admitidas potencialmente.
- La cantidad de VF que se admiten en una NIC Intel puede ser diferente de la cantidad admitida en una NIC Emulex. Consulte la documentación técnica del proveedor de la NIC.

- Si tiene NIC Intel y Emulex con SR-IOV habilitado, la cantidad de VF disponibles para las NIC Intel depende de la cantidad de VF que se configuren para la NIC Emulex, y viceversa. Puede calcular la cantidad máxima de VF que se pueden usar si los 3.072 vectores de interrupción están disponibles para el acceso directo mediante esta fórmula:

  ```
  3X + 2Y < 3072
  ```

  donde `X` es la cantidad de VF de Intel y `Y` es la cantidad de VF de Emulex.

  Esta cifra puede ser menor si otros tipos de dispositivos en el host usan más de 1.024 vectores de interrupción del total de 4.096 vectores del host.
- vSphere SR-IOV admite hasta 1.024 VF en una NIC Intel o Emulex admitida.
- vSphere SR-IOV admite hasta 64 VF en una NIC Intel o Emulex admitida.
- Si una NIC Intel admitida pierde la conexión, todas las VF de la NIC física interrumpen la comunicación por completo, incluso entre las VF.
- Si una NIC Emulex admitida pierde la conexión, todas las VF interrumpen la comunicación con el entorno externo, pero se conserva la comunicación entre las VF.
- Los controladores de VF ofrecen varias características, como compatibilidad con IPv6, TSO y suma de comprobación de LRO. Para obtener más información, consulte la documentación técnica del proveedor de la NIC.

DirectPath I/O frente a SR-IOV

SR-IOV ofrece beneficios de rendimiento y compensaciones similares a los de DirectPath I/O. DirectPath I/O y SR-IOV tienen una funcionalidad similar, pero se usan para lograr diferentes objetivos.

SR-IOV es beneficioso para las cargas de trabajo con tasas de paquetes muy elevadas o requisitos de latencia muy baja. Al igual que DirectPath I/O, SR-IOV no es compatible con ciertas características de virtualización de núcleo, como vMotion. No obstante, SR-IOV permite compartir un mismo dispositivo físico entre varios invitados.

Con DirectPath I/O, es posible asignar solamente una función física a una máquina virtual. SR-IOV permite compartir un mismo dispositivo físico y, de esta forma, conectar varias máquinas virtuales directamente a la función física.

Configurar una máquina virtual para utilizar SR-IOV

Para utilizar las capacidades de SR-IOV, se deben habilitar las funciones virtuales de SR-IOV en el host y conectar una máquina virtual a las funciones.

Requisitos previos

Compruebe que la configuración del entorno admita SR-IOV. Consulte la Compatibilidad con SR-IOV.

Procedimiento

1 Habilitar SR-IOV en un adaptador físico de host

Para poder conectar máquinas virtuales a funciones virtuales, primero se debe utilizar vSphere Web Client para habilitar SR-IOV y establecer la cantidad de funciones virtuales en el host.

2 Asignar una función virtual como adaptador de acceso directo de SR-IOV a una máquina virtual

Para garantizar que una máquina virtual y una NIC física puedan intercambiar datos, es necesario asociar la máquina virtual con una o varias funciones virtuales como adaptadores de red de acceso directo de SR-IOV.

Resultados

El tráfico pasa del adaptador de acceso directo de SR-IOV al adaptador físico de acuerdo con la directiva vigente sobre el puerto asociado en el conmutador estándar o distribuido.

Para examinar qué función virtual se asigna a un adaptador de red de acceso directo de SR-IOV, en la pestaña **Resumen** de la máquina virtual, expanda el panel **Hardware de máquina virtual** y revise las propiedades del adaptador.

En el diagrama de topología del conmutador, los adaptadores de la máquina virtual que utilizan funciones virtuales están marcados con el icono .

Pasos siguientes

Configure el tráfico que pasa por las funciones virtuales asociadas a la máquina virtual mediante las directivas de redes del conmutador, grupo de puertos y puerto. Consulte Opciones de redes para el tráfico relacionado con una máquina virtual con SR-IOV habilitado.

Habilitar SR-IOV en un adaptador físico de host

Para poder conectar máquinas virtuales a funciones virtuales, primero se debe utilizar vSphere Web Client para habilitar SR-IOV y establecer la cantidad de funciones virtuales en el host.

Procedimiento

1 En vSphere Web Client, desplácese hasta el host.

2 En la pestaña **Configurar**, expanda **Redes** y seleccione **Adaptadores físicos**.

Puede ver la propiedad de SR-IOV para determinar si un adaptador físico admite SR-IOV.

3 Seleccione el adaptador físico y haga clic en **Editar la configuración del adaptador**.

4 En SR-IOV, seleccione **Habilitado** en el menú desplegable **Estado**.

5 En el cuadro de texto **Cantidad de funciones virtuales**, escriba la cantidad de funciones virtuales que desea configurar para el adaptador.

   El valor "0" implica que SR-IOV no se habilita para esa función física.

6 Haga clic en **Aceptar**.

7 Reinicie el host.

Resultados

Las funciones virtuales se activan en el puerto de NIC representado por la entrada del adaptador físico. Aparecen en la lista de dispositivos de PCI en la pestaña **Configuración** del host.

Puede utilizar los comandos `esxcli network sriovnic` de vCLI para examinar la configuración de las funciones virtuales en el host.

Pasos siguientes

Asocie la máquina virtual con una función virtual a través de un adaptador de red de acceso directo de SR-IOV.

Asignar una función virtual como adaptador de acceso directo de SR-IOV a una máquina virtual

Para garantizar que una máquina virtual y una NIC física puedan intercambiar datos, es necesario asociar la máquina virtual con una o varias funciones virtuales como adaptadores de red de acceso directo de SR-IOV.

Requisitos previos

- Compruebe que en el host existan las funciones virtuales.
- Compruebe que los dispositivos de redes de acceso directo para las funciones virtuales estén activos en la lista Dispositivos PCI de la pestaña **Configuración** del host.
- Compruebe que la máquina virtual sea compatible con ESXi 5.5 y versiones posteriores.
- Compruebe que se haya seleccionado Red Hat Enterprise Linux 6 y versiones posteriores o Windows como sistema operativo invitado cuando se creó la máquina virtual.

Procedimiento

1 Ubique la máquina virtual en vSphere Web Client.

   a Seleccione un centro de datos, una carpeta, un clúster, un grupo de recursos o un host y haga clic en la pestaña **Máquinas virtuales**.

   b Haga clic en **Máquinas virtuales** y haga doble clic en la máquina virtual en la lista.

2 Apague la máquina virtual.

3 En la pestaña **Configurar** de la máquina virtual, expanda **Configuración** y seleccione **Hardware de máquina virtual**.

4 Haga clic en **Editar** y seleccione la pestaña **Hardware virtual** en el cuadro de diálogo que se muestra en la configuración.

5 Desde el menú desplegable **Nuevo dispositivo**, seleccione **Red** y haga clic en **Agregar**.

6 Expanda la sección Nueva red y conecte la máquina virtual al grupo de puertos.

   La NIC virtual no usa este grupo de puertos para el tráfico de datos. El grupo de puertos se usa para extraer las propiedades de redes, por ejemplo, el etiquetado de VLAN, y aplicarlas al tráfico de datos.

7 En el menú desplegable **Tipo de adaptador**, seleccione **Acceso directo de SR-IOV**.

8 En el menú desplegable **Función física**, seleccione el adaptador físico que funcionará como respaldo del adaptador de máquina virtual de acceso directo.

9 Para permitir cambios de la MTU de los paquetes provenientes del sistema operativo invitado, use el menú desplegable **Cambio de MTU de sistema operativo invitado**.

10 Expanda la sección Memoria, seleccione **Reservar toda la memoria de invitado (todo bloqueado)** y haga clic en **Aceptar**.

   La unidad de administración de memoria de E/S (IOMMU) debe tener comunicación con la totalidad de la memoria de la máquina virtual para que el dispositivo de acceso directo tenga acceso a la memoria a través del acceso de memoria directo (DMA).

11 Encienda la máquina virtual.

Resultados

Cuando se enciende la máquina virtual, el host ESXi selecciona una función virtual libre del adaptador físico y la asigna al adaptador de acceso directo de SR-IOV. El host valida todas las propiedades del adaptador de máquina virtual y la función virtual subyacente respecto de la configuración del grupo de puertos al cual pertenece la máquina virtual.

Opciones de redes para el tráfico relacionado con una máquina virtual con SR-IOV habilitado

En vSphere 5.5 y versiones posteriores, puede configurar ciertas características de redes en un adaptador de máquina virtual que tenga una función virtual (VF) asociada. Use las opciones de configuración del conmutador, el grupo de puertos o el puerto en función del tipo de conmutador virtual (estándar o distribuido) que controla el tráfico.

Tabla 10-2. Opciones de redes para un adaptador de máquina virtual que usa una VF

Opción de redes	Descripción
Tamaño de MTU	Cambie el tamaño del MTU, por ejemplo, para habilitar las tramas gigantes.
Directiva de seguridad para el tráfico de VF	■ Si el sistema operativo invitado cambia la dirección MAC inicial de un adaptador de red de máquina virtual que usa una VF, acepte o descarte las tramas entrantes para la nueva dirección mediante la opción **Cambios de dirección MAC**. ■ Habilite el modo promiscuo global para los adaptadores de red de máquina virtual, incluidos los adaptadores que usan VF.
Modo de etiquetado de VLAN	Configure el etiquetado de VLAN en el conmutador estándar o distribuido; es decir, habilite el modo Etiquetado de conmutador de VLAN o permita que el tráfico etiquetado llegue a las máquinas virtuales asociadas con VF, es decir, habilite la opción Etiquetado de invitado virtual.

Usar un adaptador físico de SR-IOV para controlar el tráfico de una máquina virtual

En vSphere 5.5 y versiones posteriores, tanto la función física (Physical Function, PF) como las funciones virtuales (Virtual Functions, VF) de un adaptador físico compatible con SR-IOV pueden configurarse para controlar el tráfico de máquina virtual.

La PF de un adaptador físico SR-IOV controla las VF que usan las máquinas virtuales y pueden transportar el tráfico que pasa por el conmutador estándar o distribuido que controla las redes de estas máquinas virtuales compatibles con SR-IOV.

El adaptador físico de SR-IOV funciona con diferentes modos, en función de si se hace una copia de seguridad del tráfico del conmutador.

Modo mixto

El adaptador físico proporciona funciones virtuales a las máquinas virtuales asociadas al conmutador y controla directamente el tráfico desde las máquinas virtuales no SR-IOV del conmutador.

Puede comprobar si un adaptador físico de SR-IOV funciona en modo mixto en el diagrama de topología del conmutador. Un adaptador físico de SR-IOV en modo mixto se muestra con el icono  en la lista de adaptadores físicos para un conmutador estándar o en la lista de adaptadores del grupo de vínculo superior para un conmutador distribuido.

Modo de solo SR-IOV

El adaptador físico proporciona funciones virtuales a las máquinas virtuales conectadas a un conmutador virtual, pero no controla el tráfico desde las máquinas virtuales no SR-IOV del conmutador.

Para comprobar si el adaptador físico está en el modo de solo SR-IOV, examine el diagrama de topología del conmutador. En este modo, el adaptador físico está en una lista independiente denominada Adaptadores externos de SR-IOV y aparece con el icono .

Modo no SR-IOV

El adaptador físico no se usa para el tráfico relacionado con las máquinas virtuales que admiten VF. Controla el tráfico únicamente de las máquinas virtuales no SR-IOV.

Habilitar SR-IOV mediante perfiles de host o un comando ESXCLI

Es posible configurar las funciones virtuales en un host ESXi utilizando un comando ESXCLI o utilizando un perfil de host para configurar varios hosts de manera simultánea o para configurar hosts sin estado.

Habilitar SR-IOV en un perfil de host

Para varios hosts o para un host sin estado, puede configurar las funciones virtuales de la NIC física mediante un perfil de host y aplicar el perfil a un host con Auto Deploy.

Para obtener información sobre la ejecución de ESXi mediante Auto Deploy con perfiles de host, consulte la documentación *Instalar y configurar vCenter Server*.

También puede habilitar las funciones virtuales de SR-IOV en el host mediante el uso del comando vCLI `esxcli system module parameters set` en el parámetro del controlador de NIC correspondiente a las funciones virtuales de acuerdo con la documentación del controlador. Para obtener más información sobre cómo utilizar los comandos vCLI, consulte la *documentación de vSphere Command-Line Interface*.

Requisitos previos

- Compruebe que la configuración del entorno admita SR-IOV. Consulte la Compatibilidad con SR-IOV.
- Cree un perfil de host basado en el host compatible con SR-IOV. Consulte la documentación de *vSphere Host Profiles*.

Procedimiento

1 En la página de inicio de vSphere Web Client, haga clic en **Perfiles de host**.

2 Seleccione el perfil de host de la lista y haga clic en la pestaña **Configurar**.

3 Haga clic en **Editar perfil de host** y expanda el nodo **Configuración general del sistema**.

4 Para crear funciones virtuales, expanda **Parámetro de módulo kernel** y seleccione el parámetro del controlador de la función física.

   Por ejemplo, el parámetro para el controlador de función física de una NIC física Intel es `max_vfs`.

5 En el cuadro de texto **Valor**, escriba una lista separada por comas de números de función virtuales válidos.

Cada entrada de la lista indica la cantidad de funciones virtuales que se desea configurar para cada función física. El valor "0" garantiza que SR-IOV no esté habilitado para esa función física.

Por ejemplo, si hay un puerto doble, establezca el valor en `x,y`, donde *x* o *y* representa la cantidad de funciones virtuales que desea habilitar para un mismo puerto.

Si la cantidad de destino de las funciones virtuales en un único host es 30, es posible que dos tarjetas de puerto doble estén establecidas en `0,10,10,10`.

Nota La cantidad de funciones virtuales compatibles y disponibles para la configuración depende de la configuración del sistema.

6 Haga clic en **Finalizar**.

7 Corrija el perfil de host según corresponda para el host.

Resultados

Las funciones virtuales aparecen en la lista de dispositivos de PCI en la pestaña **Configuración** del host.

Pasos siguientes

Asocie una función virtual con un adaptador de máquina virtual a través del tipo de adaptador de red de acceso directo de SR-IOV. Consulte Asignar una función virtual como adaptador de acceso directo de SR-IOV a una máquina virtual.

Habilitar SR-IOV en un adaptador físico de host mediante un comando ESXCLI

En ciertas situaciones de solución de problemas o para configurar hosts directamente, puede ejecutar un comando de consola en ESXi a fin de crear funciones virtuales de SR-IOV en un adaptador físico.

Para crear funciones virtuales de SR-IOV en el host, manipule el parámetro del controlador de NIC para las funciones virtuales según se indica en la documentación del controlador.

Requisitos previos

Instale el paquete de vCLI, implemente la máquina virtual de vSphere Management Assistant (vMA) o use ESXi Shell. Consulte *Introducción a vSphere Command-Line Interface*.

Procedimiento

1 Para crear funciones virtuales, establezca el parámetro de las funciones virtuales en el controlador de NIC y ejecute el comando `esxcli system module parameters set` en el símbolo del sistema.

```
esxcli system    module parameters set -m driver -p vf_param=w,x,y,z
```

Donde *driver* es el nombre del controlador de NIC y *vf_param* es el parámetro específico del controlador para crear la función virtual.

Puede usar una lista separada por comas para establecer los valores del parámetro *vf_param*, donde cada entrada indica la cantidad de funciones virtuales de un puerto. El valor "0" garantiza que SR-IOV no esté habilitado para esa función física.

Si existen dos NIC de puerto doble, puede establecer el valor en `w,x,y,z`, donde *w*,*x*,*y* y *z* representan la cantidad de funciones virtuales que se desean habilitar para un puerto. Por ejemplo, para crear 30 funciones virtuales distribuidas en dos tarjetas Intel de puerto doble con el controlador ixgbe, ejecute el siguiente comando para el controlador ixgbe y el parámetro `max_vfs`:

```
esxcli system module parameters set -m ixgbe -p max_vfs=0,10,10,10
```

2 Reinicie el host para crear las funciones virtuales.

Pasos siguientes

Asocie una función virtual con un adaptador de máquina virtual a través del tipo de adaptador de red de acceso directo de SR-IOV. Consulte Asignar una función virtual como adaptador de acceso directo de SR-IOV a una máquina virtual.

Una máquina virtual que utiliza una función virtual de SR-IOV no se enciende debido a que el host está fuera de los vectores de interrupción

En un host ESXi, una o más máquinas virtuales que usan funciones virtuales (VF) de SR-IOV para redes están apagadas.

Problema

En un host ESXi, una o más máquinas virtuales que utilizan funciones virtuales (VF) de SR-IOV para redes no se encienden si el número total de funciones virtuales asignadas está cerca del número máximo de VF especificadas en la guía *Valores máximos de configuración de vSphere*.

El archivo de registro de la máquina virtual `vmware.log` contiene el siguiente mensaje sobre la VF:

```
PCIPassthruChangeIntrSettings: vf_name failed to register interrupt (error code 195887110)
```

El archivo de registro de VMkernel `vmkernel.log` contiene los siguientes mensajes sobre el VF asignado a la máquina virtual:

```
VMKPCIPassthru: 2565: BDF = vf_name intrType = 4 numVectors: 3
WARNING: IntrVector: 233: Out of interrupt vectors
```

Causa

La cantidad de vectores de interrupción asignables escala con la cantidad de CPU físicas en un host ESXi. Un host ESXi que posee 32 CPU puede proporcionar un total de 4.096 vectores de interrupción. Cuando el host arranca, los dispositivos en el host, como controladoras de almacenamiento, adaptadores de red físicos y controladoras USB, consumen una subred de 4.096 vectores. Si estos dispositivos requieren más de 1.024 vectores, se reduce la cantidad máxima de VF que se admite potencialmente.

Cuando una máquina virtual se enciende y se inicia el controlador de VF del sistema operativo invitado, se consumen vectores de interrupción. Si la cantidad de vectores de interrupción no está disponible, el sistema operativo invitado se apaga inesperadamente sin mensajes de error.

Actualmente no existe una regla para determinar la cantidad de vectores de interrupción que se consumen o que hay disponibles en un host. Esta cantidad depende de la configuración del hardware del host.

Solución

- Para poder encender las máquinas virtuales, reduzca la cantidad total de VF asignadas a máquinas virtuales en el host.

  Por ejemplo, cambie el adaptador de red de SR-IOV de una máquina virtual a un adaptador que esté conectado a vSphere Standard Switch o vSphere Distributed Switch.

Acceso de memoria directo remoto para máquinas virtuales

vSphere 6.5 y versiones posteriores admiten la comunicación de acceso de memoria directo remoto (Remote Direct Memory Access, RDMA) entre máquinas virtuales que tienen adaptadores de red de RDMA paravirtualizado (PVRDMA).

Descripción general de RDMA

RDMA permite el acceso de memoria de la memoria de un equipo a la memoria de otro equipo sin involucrar el sistema operativo ni la CPU. La transferencia de memoria se descarga en los adaptadores de canal de host (HCA) compatibles con RDMA. Un adaptador de red de PVRDMA proporciona acceso de memoria directo remoto en un entorno virtual.

Usar RDMA en vSphere

En vSphere, una máquina virtual puede usar un adaptador de red de PVRDMA para comunicarse con otras máquinas virtuales que tienen dispositivos de PVRDMA. Dichas máquinas virtuales deben estar conectadas a la misma instancia de vSphere Distributed Switch.

El dispositivo de PVRDMA selecciona automáticamente el método de comunicación entre las máquinas virtuales. Para las máquinas virtuales que se ejecutan en el mismo host ESXi con o sin un dispositivo de RDMA físico, la transferencia de datos es un memcpy entre las dos máquinas virtuales. El hardware de RDMA físico no se usa en este caso.

Para las máquinas virtuales que residen en diferentes hosts ESXi y que tienen conexión de RDMA física, los dispositivos de RDMA físicos deben tener vínculos superiores en el conmutador distribuido. En este caso, la comunicación entre las máquinas virtuales mediante PVRDMA usa los dispositivos de RDMA físicos subyacentes.

Para dos máquinas virtuales que se ejecutan en diferentes hosts ESXi, cuando al menos uno de los hosts no tiene un dispositivo de RDMA físico, la comunicación recae en un canal basado en TCP y el rendimiento se reduce.

Compatibilidad con PVRDMA

vSphere 6.5 y versiones posteriores admiten PVRDMA solo en entornos con configuración específica.

Tipos de configuración compatibles

Para usar PVRDMA en vSphere 6.5, el entorno debe cumplir con varios requisitos de configuración.

Tabla 10-3. Tipos de configuración compatibles para usar PVRDMA

Componente	Requisitos
vSphere	■ Host ESXi 6.5 o versión posterior. ■ vCenter Server o vCenter Server Appliance 6.5 o versión posterior. ■ vSphere Distributed Switch.
Host físico	■ Debe ser compatible con la versión de ESXi.
Adaptador de canal de host (HCA)	■ Debe ser compatible con la versión de ESXi. **Nota** Las máquinas virtuales que residen en diferentes hosts ESXi requieren un HCA para utilizar RDMA. Debe asignar el HCA como un vínculo superior para vSphere Distributed Switch. PVRDMA no es compatible con la formación de equipos de NIC. El HCA debe ser el único vínculo superior en vSphere Distributed Switch. Para las máquinas virtuales en los mismos hosts ESXio las máquinas virtuales que usan la reserva basada en TCP, el HCA no es obligatorio.
Máquina virtual	■ Versión de hardware virtual 13 o posterior.
Sistema operativo invitado	■ Linux (64 bits)

Para comprobar que los hosts físicos y los HCA sean compatibles con las versiones de ESXi, consulte la *Guía de compatibilidad de VMware*.

Nota Si se intentan habilitar o configurar las características no compatibles con PVRDMA en vSphere Web Client, podría observarse un comportamiento inesperado en el entorno.

Configurar un host ESXi para PVRDMA

Configure el adaptador de VMkernel y la regla de firewall de un host ESXi para la comunicación PVRDMA.

Requisitos previos

Compruebe que el host ESXi cumpla los requisitos para PVRDMA. Consulte Compatibilidad con PVRDMA.

- Etiquetar un adaptador de VMkernel para PVRDMA

  Seleccione un adaptador de VMkernel y habilítelo para la comunicación PVRDMA.

- Habilitar las reglas de firewall para PVRDMA

  Habilite las reglas de firewall para PVRDMA en el perfil de seguridad del host ESXi.

Etiquetar un adaptador de VMkernel para PVRDMA

Seleccione un adaptador de VMkernel y habilítelo para la comunicación PVRDMA.

Procedimiento

1 En vSphere Web Client, desplácese hasta el host.

2 En la pestaña **Configurar**, expanda **Sistema**.

3 Haga clic en **Configuración avanzada del sistema**.

4 Localice `Net.PVRDMAVmknic` y haga clic en **Editar**.

5 Introduzca el valor del adaptador de VMkernel que desea usar, por ejemplo, vmk0, y haga clic en **Aceptar**.

Habilitar las reglas de firewall para PVRDMA

Habilite las reglas de firewall para PVRDMA en el perfil de seguridad del host ESXi.

Procedimiento

1 En vSphere Web Client, desplácese hasta el host.

2 En la pestaña **Configurar**, expanda **Sistema**.

3 Haga clic en **Perfil de seguridad**.

4 En la sección Firewall, haga clic en **Editar**.

5 Desplácese hasta la regla de pvrdma y seleccione la casilla junto a ella.

6 Haga clic en **Aceptar**.

Asignar un adaptador PVRDMA a una máquina virtual

Para permitir que una máquina virtual intercambie datos por medio de RDMA, debe asociarla con un adaptador de red PVRDMA.

Requisitos previos

- Compruebe que el host donde se ejecuta la máquina virtual esté configurado para RDMA. Consulte Configurar un host ESXi para PVRDMA.
- Compruebe que el host esté conectado a una instancia de vSphere Distributed Switch.
- Compruebe que la máquina virtual utilice la versión 13 del hardware virtual.
- Compruebe que el sistema operativo invitado sea una distribución Linux de 64 bits.

Procedimiento

1 Ubique la máquina virtual en vSphere Web Client.

   a Seleccione un centro de datos, una carpeta, un clúster, un grupo de recursos o un host y haga clic en la pestaña **Máquinas virtuales**.

   b Haga clic en **Máquinas virtuales** y haga doble clic en la máquina virtual en la lista.

2 Apague la máquina virtual.

3 En la pestaña **Configurar** de la máquina virtual, expanda **Configuración** y seleccione **Hardware de máquina virtual**.

4 Haga clic en **Editar** y seleccione la pestaña **Hardware virtual** en el cuadro de diálogo que se muestra en la configuración.

5 Desde el menú desplegable **Nuevo dispositivo**, seleccione **Red** y haga clic en **Agregar**.

6 Expanda la sección Nueva red y conecte la máquina virtual al grupo de puertos distribuidos.

7 En el menú desplegable **Tipo de adaptador**, seleccione PVRDMA.

8 Expanda la sección **Memoria**, seleccione **Reservar toda la memoria de invitado (todo bloqueado)** y, a continuación, haga clic en **Aceptar**.

9 Encienda la máquina virtual.

Requisitos de red para RDMA over Converged Ethernet

RDMA over Converged Ethernet garantiza una comunicación RDMA de baja latencia, peso liviano y alta capacidad de proceso por medio de una red Ethernet. RoCE requiere una red que esté configurada para tráfico sin pérdida de información solo en la Capa 2 o en las Capas 2 y 3.

RDMA over Converged Ethernet (RoCE) es un protocolo de red que utiliza RDMA con el fin de ofrecer una transferencia de datos más rápida para aplicaciones de uso intensivo de la red. RoCE permite una transferencia de memoria directa entre hosts sin involucrar a las CPU de los hosts.

Hay dos versiones del protocolo RoCE. RoCE v1 funciona en la capa de red de vínculo (Capa 2). RoCE v2 funciona en la capa de red de Internet (Capa 3). Tanto RoCE v1 como RoCE v2 requieren una configuración de red sin pérdida. RoCE v1 requiere una red de Capa 2 sin pérdida, mientras que RoCE v2 requiere que las Capas 2 y 3 estén configuradas para un funcionamiento sin pérdida.

Red de Capa 2 sin pérdida

Para garantizar un entorno de Capa 2 sin pérdida, debe poder controlar los flujos de tráfico. Para lograr el control del flujo, debe habilitarse la pausa global en toda la red, o bien debe utilizarse el protocolo Priority Flow Control (PFC) definido por el grupo Data Center Bridging (DCB). PFC es un protocolo de Capa 2 que usa la clase de campo de servicios de la etiqueta 802.1Q VLAN para establecer prioridades de tráfico individuales. Coloca en pausa la transferencia de paquetes hacia un receptor de acuerdo con la clase individual de prioridades de servicio. De esta manera, un solo vínculo transporta tráfico RoCE sin pérdida y otro tipo de tráfico con pérdida, de mejor esfuerzo. En caso de congestiones en el flujo de tráfico, el tráfico con pérdida importante puede verse afectado. Para aislar diferentes flujos entre sí, utilice RoCE en una VLAN habilitada para tráfico prioritario.

Red de Capa 3 sin pérdida

RoCE v2 requiere que la transferencia de datos sin pérdida se conserve en dispositivos de enrutamiento de Capa 3. Para habilitar la transferencia de prioridades sin pérdida de PFC de Capa 2 en enrutadores de Capa 3, configure el enrutador para que asigne la configuración de prioridad recibida de un paquete a la configuración de calidad de servicio de Differentiated Serviced Code Point (DSCP) correspondiente que funciona en la Capa 3. Los paquetes de RDMA transferidos se marcan con DSCP de Capa 3, Priority Code Points (PCP) de Capa 2, o ambos. Los enrutadores utilizan DSCP o PCP para extraer la información de prioridad del paquete. En caso de que se utilice PCP, el paquete debe contener una etiqueta de VLAN, y el enrutador debe copiar los bits de PCP de la etiqueta y reenviarlos a la próxima red. Si el paquete se marca con DSCP, el enrutador debe conservar los bits de DSCP sin modificaciones.

Al igual que RoCE v1, RoCE v2 debe ejecutarse en una VLAN habilitada para prioridad de PFC.

Nota No se deben formar equipos de NIC de RoCE si se pretende utilizar RDMA en esas NIC.

Para obtener información de configuración específica del proveedor, consulte la documentación oficial del proveedor del dispositivo o conmutador respectivos.

Tramas gigantes

Las tramas gigantes permiten que los hosts ESXi envíen tramas más grandes hacia la red física. La red debe ser compatible con las tramas gigantes de un extremo al otro, incluidos los adaptadores de red, los conmutadores físicos y los dispositivos de almacenamiento.

Antes de habilitar las tramas gigantes, consulte al proveedor de hardware para confirmar que el adaptador de red físico admite tramas gigantes.

Puede habilitar las tramas gigantes en un conmutador distribuido de vSphere o en un conmutador estándar de vSphere si modifica la unidad de transmisión máxima (MTU) y le asigna un valor mayor que 1.500 bytes. El tamaño máximo de trama configurable es de 9.000 bytes.

Habilitar tramas gigantes en vSphere Distributed Switch

Puede habilitar las tramas gigantes para todo el tráfico que pasa por vSphere Distributed Switch.

Importante Al cambiar el tamaño de MTU de una instancia de vSphere Distributed Switch, las NIC físicas que se asignan como vínculos superiores se desactivan y se vuelven a activar. Debido a esto, la red se interrumpe brevemente (de 5 a 10 milisegundos) para las máquinas virtuales o los servicios que utilizan los vínculos superiores.

Procedimiento

1. En vSphere Web Client, desplácese hasta el conmutador distribuido.
2. En la pestaña **Configurar**, expanda **Configuración** y seleccione **Propiedades**.
3. Haga clic en **Editar**.
4. Haga clic en **Opciones avanzadas** y establezca la propiedad **MTU** con un valor mayor que 1.500 bytes.

   El valor máximo para el tamaño de MTU es de 9.000 bytes.
5. Haga clic en **Aceptar**.

Habilitar tramas gigantes en vSphere Standard Switch

Habilite las tramas gigantes para todo el tráfico a través de vSphere Standard Switch en un host.

Procedimiento

1. En vSphere Web Client, desplácese hasta el host.
2. En la pestaña **Configurar**, expanda **Redes** y seleccione **Conmutadores virtuales**.
3. Seleccione un conmutador estándar de la tabla de conmutadores virtuales y haga clic en **Editar configuración**.
4. En la sección **Propiedades**, configure la propiedad **MTU** con un valor superior a 1.500 bytes.

   Puede aumentar el tamaño de MTU hasta 9.000 bytes.
5. Haga clic en **Aceptar**.

Habilitar tramas gigantes para un adaptador VMkernel

Las tramas gigantes reducen la carga de CPU originada por la transferencia de datos. Para habilitar las tramas gigantes en un adaptador VMkernel, cambie las unidades de transmisión máximas (MTU) del adaptador.

Procedimiento

1. En vSphere Web Client, desplácese hasta el host.
2. En la pestañaConfigurar**Configurar**, expanda **Redes** y seleccione **Adaptadores de VMKernel**.

3 Seleccione un adaptador VMkernel de la tabla de adaptadores.

   Aparecen las propiedades del adaptador.

4 Haga clic en el nombre del adaptador VMkernel.

5 Haga clic en **Editar**.

6 Seleccione **Configuración de NIC** y establezca la propiedad **MTU** con un valor mayor que 1.500.

   Puede aumentar el tamaño de MTU hasta 9.000 bytes.

7 Haga clic en **Aceptar**.

Habilitar la compatibilidad con tramas gigantes en una máquina virtual

Para habilitar la compatibilidad con tramas gigantes en una máquina virtual se requiere un adaptador vmxnet mejorado para esa máquina virtual.

Procedimiento

1 Ubique la máquina virtual en vSphere Web Client.

   a Seleccione un centro de datos, una carpeta, un clúster, un grupo de recursos o un host y haga clic en la pestaña **Máquinas virtuales**.

   b Haga clic en **Máquinas virtuales** y haga doble clic en la máquina virtual en la lista.

2 En la pestaña **Configurar** de la máquina virtual, expanda **Configuración** y seleccione **Hardware de máquina virtual**.

3 Haga clic en **Editar** y seleccione la pestaña **Hardware virtual** en el cuadro de diálogo que se muestra en la configuración.

4 Expanda la sección **Adaptador de red**. Registre la configuración de red y la dirección MAC que utiliza el adaptador de red.

5 Haga clic en **Quitar** para quitar el adaptador de red de la máquina virtual.

6 Desde el menú desplegable **Nuevo dispositivo**, seleccione **Red** y haga clic en **Agregar**.

7 Desde el menú desplegable **Tipo de adaptador**, seleccione **VMXNET 2 (mejorado)** o **VMXNET 3**.

8 Establezca la configuración de red a las opciones registradas para el adaptador de red antiguo.

9 Establezca **Dirección MAC** en **Manual** y escriba la dirección MAC que estaba utilizando el adaptador de red antiguo.

10 Haga clic en **Aceptar**.

Pasos siguientes

- Compruebe que el adaptador VMXNET mejorado esté conectado a un conmutador estándar o a un conmutador distribuido que tenga habilitadas las tramas gigantes.
- En el sistema operativo invitado, configure el adaptador de red para permitir las tramas gigantes. Consulte la documentación del sistema operativo invitado.
- Configure todos los conmutadores físicos y cualquier máquina virtual o física a la que se conecte esta máquina virtual para admitir tramas gigantes.

descarga de segmentación de TCP

Utilice la descarga de segmentación de TCP (TSO) en los adaptadores de red VMkernel y las máquinas virtuales para mejorar el rendimiento de red en cargas de trabajo que tienen requisitos de latencia severa.

La TSO en la ruta de acceso de transmisión de los adaptadores de red físicos y los adaptadores de red VMkernel y de la máquina virtual mejora el rendimiento de los hosts ESXi, puesto que reduce la sobrecarga de las operaciones de red TCP/IP en la CPU. Cuando se habilita la TSO, el adaptador de red divide los grupos de datos más grandes en segmentos TCP en lugar de la CPU. El VMkernel yel sistema operativo invitado puedenutilizar más ciclos de CPU para ejecutar las aplicaciones.

Para obtener los beneficios de mejora del rendimiento que proporciona la TSO, habilítela en toda la ruta de acceso de datos de un host ESXi, incluidos los adaptadores de red físicos, VMkernel y el sistema operativo invitado. La TSO está habilitada de forma predeterminada en el VMkernel del host ESXi y en los adaptadores VMXNET 2 y VMXNET 3 de la máquina virtual.

Para obtener información sobre la ubicación de la segmentación de paquetes TCP en la ruta de acceso de datos, consulte el artículo de la base de conocimientos de VMware de descripción de la descarga de segmentación de TCP (TSO) y la descarga de recepción grande (LRO) en un entorno de VMware.

Habilitar o deshabilitar la TSO de software en el VMkernel

Si un adaptador de red físico tiene problemas con la TSO, puede habilitar temporalmente la simulación de software de TSO en el VMkernel hasta que solucione los problemas.

Procedimiento

- Ejecute estos comandos de consola `esxcli network nic software set` para habilitar o deshabilitar la simulación de software de TSO en el VMkernel.
  - Habilite la simulación de software de TSO en el VMkernel.

    ```
    esxcli network nic software set --ipv4tso=1 -n vmnicXesxcli network nic software set
    --ipv6tso=1 -n vmnicX
    ```

- Deshabilite la simulación de software de TSO en el VMkernel.

  ```
  esxcli network nic software set --ipv4tso=0 -n vmnicXesxcli network nic software set
  --ipv6tso=0 -n vmnicX
  ```

  donde *X* en vmnic*X* representa la cantidad de puertos de NIC en el host.

  El cambio de configuración se conserva aunque se reinicie el host.

Determinar si los adaptadores de red físicos de un host ESXi admiten TSO

Examine si un adaptador de red físico descarga la segmentación de paquetes TCP/IP cuando calcule el rendimiento de redes en un host que procese cargas de trabajo sujetas a la latencia. Si el adaptador de red físico admite TSO, la TSO está habilitada de forma predeterminada.

Procedimiento

- Ejecute el siguiente comando de consola para determinar si la TSO está habilitada en los adaptadores de red físicos de un host.

  ```
  esxcli network nic tso get
  ```

Habilitar o deshabilitar la TSO en un host ESXi

Habilite la descarga de segmentación de TCP (TSO) en la ruta de transmisión si desea que la NIC divida los fragmentos de datos en segmentos de TCP. Deshabilite la TSO si desea que la CPU ejecute la segmentación de TCP.

De forma predeterminada, el host usa la TSO de hardware si los adaptadores físicos admiten esta función.

Procedimiento

1. En vSphere Web Client, desplácese hasta el host.
2. En la pestaña **Configurar**, expanda **Sistema**.
3. Haga clic en **Configuración avanzada del sistema**.
4. Edite el valor del parámetro `Net.UseHwTSO` para IPv4 y de `Net.UseHwTSO6` para IPv6.
   - Para habilitar la TSO, configure `Net.UseHwTSO` y `Net.UseHwTSO6` en **1**.
   - Para deshabilitar la TSO, configure `Net.UseHwTSO` y `Net.UseHwTSO6` en **0**.
5. Haga clic en **Aceptar** para aplicar los cambios.

6 Para volver a cargar el módulo de controlador del adaptador físico, ejecute el comando de consola `esxcli system module set` en ESXi Shell del host.

   a Para deshabilitar el controlador, ejecute el comando `esxcli system module set` con la opción `--enabled false`.

```
esxcli    system module set
--enabled false
--module
nic_driver_module
```

   b Para habilitar el controlador, ejecute el comando `esxcli system module set` con la opción `--enabled true`.

```
esxcli    system module set
--enabled true
--module
nic_driver_module
```

Resultados

Si un adaptador físico no admite la TSO de hardware, el VMkernel segmenta los paquetes de TCP de mayor tamaño provenientes del sistema operativo invitado y los envía al adaptador.

Determinar si la TSO está habilitada en un host ESXi

Examine si la TSO de hardware está habilitada en el VMkernel cuando calcule el rendimiento de redes en un host donde se ejecutan cargas de trabajo sujetas a latencia. De forma predeterminada, la TSO de hardware está habilitada en un host ESXi.

Procedimiento

1 En vSphere Web Client, desplácese hasta el host.

2 En la pestaña **Configurar**, expanda **Sistema**.

3 Haga clic en **Configuración avanzada del sistema**.

4 Examine el valor de los parámetros `Net.UseHwTSO` y `Net.UseHwTSO6`.

   `Net.UseHwTSO` muestra el estado de TSO para IPv4, y `Net.UseHwTSO6` hace lo mismo para IPv6. La TSO está habilitada si la propiedad está configurada en 1.

Habilitar o deshabilitar TSO en una máquina virtual de Linux

Habilite la compatibilidad con TSO en el adaptador de red de una máquina virtual de Linux de modo que el sistema operativo invitado redirija al VMkernel los paquetes TCP que necesitan segmentarse.

Requisitos previos

- Compruebe que ESXi 6.0 sea compatible con el sistema operativo invitado Linux.

  Consulte la documentación de *Guía de compatibilidad de VMware*.

- Compruebe que el adaptador de red de la máquina virtual de Linux sea VMXNET2 o VMXNET3.

Procedimiento

- ◆ Para habilitar o deshabilitar la TSO en una ventana de terminal del sistema operativo invitado Linux, ejecute el comando `ethtool` con las opciones `-K` y `tso`.

  - Para habilitar la TSO, ejecute el siguiente comando:

    ```
    ethtool-K ethYtsoon
    ```

  - Para deshabilitar la TSO, ejecute el siguiente comando:

    ```
    ethtool-K ethYtsooff
    ```

  donde *Y* en eth*Y* es el número de secuencia de la NIC en la máquina virtual.

Habilitar o deshabilitar TSO en una máquina virtual de Windows

De forma predeterminada, TSO se habilita en los adaptadores de red VMXNET2 y VXMNET3 de las máquinas virtuales de Windows. Por motivos de rendimiento, deshabilitar TSO puede resultar útil.

Requisitos previos

- Compruebe que ESXi 6.0 sea compatible con el sistema operativo invitado Windows. Consulte la documentación de *Guía de compatibilidad de VMware*.
- Compruebe que el adaptador de red de la máquina virtual de Windows sea VMXNET2 o VMXNET3.

Procedimiento

1. En el panel de control de Windows, en la opción Centro de redes y recursos compartidos, haga clic en el nombre del adaptador de red.
2. Haga clic en el nombre.

   Se muestra un cuadro de diálogo con el estado del adaptador.
3. Haga clic en **Propiedades** y, debajo del tipo de adaptador de red, haga clic en **Configurar**.
4. En la pestaña **Opciones avanzadas**, establezca las propiedades **Descarga de envío grande V2 (IPv4)** y **Descarga de envío grande V2 (IPv6)** en **Habilitado** o **Deshabilitado**.
5. Haga clic en **Aceptar**.
6. Reinicie la máquina virtual.

descarga de recepción grande

Utilice la descarga de recepción grande (LRO) para reducir la sobrecarga de CPU para el procesamiento de paquetes que llegan desde la red a alta velocidad.

La LRO vuelve a ensamblar los paquetes de red entrantes en búferes de mayor tamaño y transmite los paquetes resultantes, más grandes pero en menor cantidad, a la pila de red del host o la máquina virtual. La CPU entonces debe procesar menos paquetes que cuando la LRO está deshabilitada, por lo que el uso de redes es menor, especialmente en el caso de conexiones con ancho de banda elevado.

Para aprovechar la mejora del rendimiento de la LRO, habilite esta función en toda la ruta de acceso de datos de un host ESXi, incluido el VMkernel y el sistema operativo invitado. De forma predeterminada, la LRO está habilitada en el VMkernel y en los adaptadores de máquina virtual VMXNET3.

Para obtener información sobre la ubicación de la adición de paquetes TCP en la ruta de acceso de datos, consulte el artículo de la base de conocimientos de VMware de descripción de la descarga de segmentación de TCP (TSO) y la descarga de recepción grande (LRO) en un entorno de VMware.

Habilitar la LRO de hardware para todos los adaptadores de VMXNET3 en un host ESXi

Habilite las capacidades de hardware de los adaptadores físicos del host para combinar paquetes TCP entrantes para los adaptadores de máquina virtual VXMNET3 mediante el uso de la tecnología LRO en vez de consumir recursos para el montaje en el sistema operativo invitado.

Procedimiento

1 En vSphere Web Client, desplácese hasta el host.

2 En la pestaña **Configurar**, expanda **Sistema**.

3 Haga clic en **Configuración avanzada del sistema**.

4 Edite el valor del parámetro `Net.Vmxnet3HwLRO`.

- Para habilitar la LRO de hardware, establezca `Net.Vmxnet3HwLRO` en **1**.
- Para deshabilitar la LRO de hardware, establezca `Net.Vmxnet3HwLRO` en **0**.

5 Haga clic en **Aceptar** para aplicar los cambios.

Habilitar o deshabilitar la LRO de software para todos los adaptadores VMXNET3 en un host ESXi

Utilice la LRO de software en el back-end del VMkernel de los adaptadores VMXNET3 para mejorar el rendimiento de redes de las máquinas virtuales si los adaptadores físicos del host no admiten la LRO de hardware.

vSphere 5.5 y versiones posteriores admiten la LRO de software para los paquetes IPv4 e IPv6.

Requisitos previos

Procedimiento

1 En vSphere Web Client, desplácese hasta el host.

2 En la pestaña **Configurar**, expanda **Sistema**.

3 Haga clic en **Configuración avanzada del sistema**.

4 Edite el valor del parámetro `Net.Vmxnet3SwLRO` para los adaptadores VMXNET3.

- Para habilitar la LRO de software, establezca `Net.Vmxnet3SwLRO` en 1.
- Para deshabilitar la LRO de software, establezca `Net.Vmxnet3SwLRO` en 0.

5 Haga clic en **Aceptar** para aplicar los cambios.

Determinar si LRO está habilitada para los adaptadores de VMXNET3 en un host ESXi

Examine el estado de LRO en ESXi cuando calcule el rendimiento de la red en un host donde se ejecutan cargas de trabajo sujetas a latencia.

Requisitos previos

Procedimiento

1 En vSphere Web Client, desplácese hasta el host.

2 En la pestaña **Configurar**, expanda **Sistema**.

3 Haga clic en **Configuración avanzada del sistema**.

4 Examine el valor de los parámetros de LRO para VMXNET2 y VMXNET3.

- Para la funcionalidad LRO de hardware, examine el parámetro `Net.Vmxnet3HwLRO`. Si es igual a 1, la funcionalidad de LRO de hardware está habilitada.
- Para la funcionalidad LRO de software, examine el parámetro `Net.Vmxnet3SwLRO`. Si es igual a 1, la funcionalidad de LRO de hardware está habilitada.

Cambiar tamaño del búfer de la LRO para los adaptadores VMXNET 3

Puede cambiar el tamaño del búfer para la adición de paquetes de las conexiones de máquina virtual a través de adaptadores de red VMXNET 3. Aumente el tamaño del búfer para reducir la cantidad de confirmaciones de TCP y mejorar la eficacia de las cargas de trabajo.

Procedimiento

1 En vSphere Web Client, desplácese hasta el host.

2 En la pestaña **Configurar**, expanda **Sistema**.

3 Haga clic en **Configuración avanzada del sistema**.

4 Introduzca un valor entre 1 y 65535 para el parámetro `Net.VmxnetLROMaxLength` a fin de establecer el tamaño del búfer de la LRO en bytes.

   El tamaño predeterminado del búfer de la LRO equivale a 32.000 bytes.

Habilitar o deshabilitar la LRO para todos los adaptadores VMkernel en un host ESXi

Usar la LRO en los adaptadores de red VMkernel en un host ESXi permite mejorar el rendimiento de las redes para el tráfico de infraestructura entrante.

Procedimiento

1 En vSphere Web Client, desplácese hasta el host.

2 En la pestaña **Configurar**, expanda **Sistema**.

3 Haga clic en **Configuración avanzada del sistema**.

4 Edite el valor del parámetro `Net.TcpipDefLROEnabled`.

   - Para habilitar la LRO para los adaptadores de red VMkernel del host, establezca `Net.TcpipDefLROEnabled` en **1**.
   - Para deshabilitar la LRO de software para los adaptadores de red VMkernel del host, establezca `Net.TcpipDefLROEnabled` en **0**.

5 Haga clic en **Aceptar** para aplicar los cambios.

Cambiar tamaño del búfer de la LRO para los adaptadores VMkernel

Puede modificar el tamaño del búfer para la adición de paquetes de las conexiones VMkernel. Aumente el tamaño del búfer para reducir la cantidad de confirmaciones de TCP y mejorar la eficacia del VMkernel.

Procedimiento

1 En vSphere Web Client, desplácese hasta el host.

2 En la pestaña **Configurar**, expanda **Sistema**.

3 Haga clic en **Configuración avanzada del sistema**.

4 Introduzca un valor entre 1 y 65535 para el parámetro `Net.TcpipDefLROMaxLength` a fin de establecer el tamaño del búfer de la LRO en bytes.

   El tamaño predeterminado del búfer de la LRO equivale a 32768 bytes.

Habilitar o deshabilitar la LRO en un adaptador VMXNET3 en una máquina virtual de Linux

Si la LRO está habilitada en los adaptadores VMXNET3 del host, active la compatibilidad con LRO en un adaptador de red de una máquina virtual Linux para garantizar que el sistema operativo invitado no gaste recursos para combinar los paquetes entrantes en búferes más grandes.

Requisitos previos

Compruebe que el kernel Linux sea 2.6.24 o posterior.

Procedimiento

- En una ventana de terminal del sistema operativo invitado Linux, ejecute el comando `ethtool` con las opciones `-K` y `lro`.
  - Para habilitar la LRO, ejecute el siguiente comando:

    ```
    ethtool-K ethYlroon
    ```

    donde *Y* en eth*Y* es el número de secuencia de la NIC en la máquina virtual.
  - Para deshabilitar la LRO, ejecute el siguiente comando:

    ```
    ethtool-K ethYlrooff
    ```

    donde *Y* en eth*Y* es el número de secuencia de la NIC en la máquina virtual.

Habilitar o deshabilitar la LRO en un adaptador VMXNET3 en una máquina virtual de Windows

Si se habilita la LRO para adaptadores VMXNET3 en el host, active la compatibilidad con LRO en un adaptador de red de una máquina virtual de Windows para garantizar que el sistema operativo invitado no emplee recursos en combinar paquetes entrantes a búferes más grandes.

En Windows, la tecnología LRO también se denomina Fusión de segmentos de recepción (RSC).

Requisitos previos

- Compruebe que la máquina virtual ejecute Windows Server 2012 o una versión posterior y Windows 8 o una versión posterior.
- Compruebe que la máquina virtual sea compatible con ESXi 6.0 y versiones posteriores.
- Compruebe que la versión del controlador VMXNET3 instalado en el sistema operativo invitado sea 1.6.6.0 o una versión posterior.
- Compruebe que la LRO esté habilitada globalmente en una máquina virtual que ejecuta Windows Server 2012 o una versión posterior o Windows 8 o una versión posterior. Consulte Habilitar la LRO en forma global en una máquina virtual de Windows.

Procedimiento

1 En la carpeta **Centro de redes y recursos compartidos** del panel de control del sistema operativo invitado, haga clic en el nombre del adaptador de red.

  Se muestra un cuadro de diálogo con el estado del adaptador.

2 Haga clic en **Propiedades** y, debajo del tipo de adaptador de red VMXNET3, haga clic en **Configurar**.

3 En la pestaña **Opciones avanzadas**, establezca las opciones **Fusión de segmentos de recepción (IPv4)** y **Fusión de segmentos de recepción (IPv6)** en **Habilitada** o **Deshabilitada**.

4 Haga clic en **Aceptar**.

Habilitar la LRO en forma global en una máquina virtual de Windows

Para utilizar la LRO en un adaptador de VMXNET3 de una máquina virtual que ejecuta Windows 8 y versiones posteriores, o bien Windows Server 2012 y versiones posteriores, es necesario habilitar la LRO globalmente en el sistema operativo invitado. En Windows, la tecnología LRO también se denomina Fusión de segmentos de recepción (RSC).

Procedimiento

1 Para comprobar si la LRO está deshabilitada globalmente en un sistema operativo invitado Windows 8 y versiones posteriores o Windows Server 2012 y versiones posteriores, ejecute el comando `netsh int tcp show global` en el símbolo del sistema.

```
netsh int tcp show global
```

  El comando muestra el estado de los parámetros globales de TCP configurados en el sistema operativo Windows 8.x.

```
TCP Global Parameters ---------------------------------------------- Receive-Side Scaling
State : enabled Chimney Offload State : disabled NetDMA State : disabled Direct Cache
Access (DCA) : disabled Receive Window Auto-Tuning Level : normal Add-On Congestion
Control Provider : none ECN Capability : disabled RFC 1323 Timestamps : disabled Initial
RTO : 3000 Receive Segment Coalescing State : disabled
```

  Si se deshabilita globalmente la LRO en la máquina con Windows 8 y versiones posteriores o Windows Server 2012, la propiedad Estado de fusión de segmentos de recepción aparece como deshabilitada.

2 Para habilitar globalmente la LRO en el sistema operativo Windows, ejecute el comando `netsh int tcp set global` en el símbolo del sistema:

```
netsh int tcp set global rsc=enabled
```

Pasos siguientes

Habilite la LRO en el adaptador de VMXNET3 en la máquina virtual con Windows 8 y versiones posteriores o Windows Server 2012. Consulte Habilitar o deshabilitar la LRO en un adaptador VMXNET3 en una máquina virtual de Windows.

NetQueue y rendimiento de redes

NetQueue aprovecha la capacidad de algunos adaptadores de red de suministrar tráfico de red al sistema a través de varias colas de recepción que se procesan por separado, lo cual permite aumentar el procesamiento a varias CPU y mejorar el rendimiento de recepción de las redes.

Habilitar NetQueue en un host

NetQueue está habilitado de forma predeterminada. Si desea usar NetQueue después de deshabilitar esta función, debe volver a habilitarla.

Requisitos previos

Procedimiento

1 En ESXi Shell del host, use el siguiente comando:

```
esxcli system settings kernel set --setting="netNetqueueEnabled" --value="TRUE"
```

2 Use el comando `esxcli module parameters set` para configurar el controlador de NIC que usará NetQueue.

   Por ejemplo, en una NIC Emulex de puerto doble, ejecute estos comandos ESXCLI para configurar el controlador con 8 colas de recepción.

```
esxcli system module parameters set -m tg3 -p force_netq=8,8
```

3 Reinicie el host.

Deshabilitar NetQueue en un host

NetQueue está habilitado de forma predeterminada.

Requisitos previos

Familiarícese con la información sobre la configuración de controladores de NIC en *Introducción a vSphere Command-Line Interface*.

Procedimiento

1 En la interfaz de línea de comandos de VMware vSphere, utilice el siguiente comando en función de la versión del host:

```
esxcli system settings kernel set --setting="netNetqueueEnabled" --value="FALSE"
```

2 Para deshabilitar NetQueue en el controlador de NIC, utilice el comando `esxcli module parameters set`.

Por ejemplo, en un puerto doble Emulex NIC, ejecute estos comandos ESXCLI para configurar el controlador con colas de recepción 1.

```
esxcli system module parameters set -m tg3 -p force_netq=1,1
```

3 Reinicie el host.

vSphere Network I/O Control

11

Utilice vSphere Network I/O Control para asignar el ancho de banda de la red a las aplicaciones fundamentales para el negocio y para resolver situaciones en las que varios tipos de tráfico compiten por recursos comunes.

- Acerca de vSphere Network I/O Control versión 3

  vSphere Network I/O Control versión 3 incorpora un mecanismo para reservar ancho de banda para el tráfico del sistema en función de la capacidad de los adaptadores físicos de un host. Esta funcionalidad permite un control detallado de los recursos en el adaptador de red de máquina virtual similar al modelo utilizado para asignar recursos de CPU y de memoria.

- Actualizar Network I/O Control a la versión 3 en vSphere Distributed Switch

  Si actualizó vSphere Distributed Switch a la versión 6.0.0 sin convertir Network I/O Control a la versión 3, puede actualizar Network I/O Control para utilizar el modelo mejorado de asignación de ancho de banda al tráfico del sistema y a máquinas virtuales individuales.

- Habilitar Network I/O Control en vSphere Distributed Switch

  Habilite la administración de recursos de red en vSphere Distributed Switch para garantizar el ancho de banda mínimo para el tráfico de sistema de las características de vSphere y el tráfico de máquina virtual.

- Asignar ancho de banda para el sistema de tráfico

  Puede configurar Network I/O Control para asignar cierta cantidad de ancho de banda al tráfico generado por vSphere Fault Tolerance, vSphere vMotion, etc.

- Asignar ancho de banda para el tráfico de la máquina virtual

  La versión 3 de Network I/O Control permite configurar los requisitos de ancho de banda de las máquinas virtuales individuales. También puede utilizar grupos de recursos de red en los que podrá asignar una cuota de ancho de banda desde la reserva agregada para el tráfico de la máquina virtual y, a continuación, asignar ancho de banda desde el grupo hasta las máquinas virtuales individuales.

- Desplazar un adaptador físico fuera del alcance de Network I/O Control

  En determinadas condiciones, puede ser necesario excluir adaptadores físicos con baja capacidad del modelo de asignación de ancho de banda de Network I/O Control versión 3.

- Trabajar con Network I/O Control versión 2

  En vSphere Distributed Switch 5.x, al igual que en vSphere Distributed Switch actualizado a 6.0 que no cuente con la actualización de Network I/O Control a la versión 3, puede asegurarse de que el tráfico del sistema y las máquinas virtuales reciban el ancho de banda que necesitan para su operación mediante el modelo de grupo de recursos de Network I/O Control versión 2.

Acerca de vSphere Network I/O Control versión 3

vSphere Network I/O Control versión 3 incorpora un mecanismo para reservar ancho de banda para el tráfico del sistema en función de la capacidad de los adaptadores físicos de un host. Esta funcionalidad permite un control detallado de los recursos en el adaptador de red de máquina virtual similar al modelo utilizado para asignar recursos de CPU y de memoria.

La versión 3 de la característica Network I/O Control ofrece un proceso mejorado de reserva y asignación de recursos de red en todo el conmutador.

Modelos de reserva de recursos de ancho de banda

Network I/O Control versión 3 admite el uso de diferentes modelos para la administración de recursos del tráfico del sistema vinculado con los servicios de infraestructura, como vSphere Fault Tolerance, y las máquinas virtuales.

Las dos categorías de tráfico son de naturaleza diferente. El tráfico del sistema está asociado estrictamente con el host ESXi. Las rutas del tráfico de red cambian cuando se migra una máquina virtual dentro del entorno. Para suministrar recursos de red a una máquina virtual independientemente del host, es posible configurar en Network I/O Control una asignación de recursos para máquinas virtuales que sea válida para el alcance de todo el conmutador distribuido.

Garantía de ancho de banda para las máquinas virtuales

Network I/O Control versión 3 suministra ancho de banda a los adaptadores de red de las máquinas virtuales a través de restricciones de recursos compartidos, reservas y límites. En función de estas restricciones, para recibir el ancho de banda suficiente, las cargas de trabajo virtualizadas dependen del control de admisión de vSphere Distributed Switch, vSphere DRS y vSphere HA. Consulte Control de admisión del ancho de banda de máquina virtual.

Network I/O Control versión 2 y versión 3 en vSphere 6.0

En vSphere 6.0, coexisten las versiones 2 y 3 de Network I/O Control. Las dos versiones implementan modelos diferentes para asignar ancho de banda a las máquinas virtuales y al tráfico del sistema. En Network I/O Control versión 2, es posible configurar la asignación de ancho de banda para las máquinas virtuales en el nivel de adaptador físico. En cambio, en la versión 3 es posible establecer la asignación de ancho de banda para las máquinas virtuales en todo el conmutador distribuido.

Cuando se actualiza un conmutador distribuido, Network I/O Control también se actualiza a la versión 3, excepto cuando se utilizan algunas de las características que no están disponibles en Network I/O Control versión 3, como el etiquetado de CoS y los grupos de recursos de red definidos por el usuario. En este caso, la diferencia entre los modelos de asignación de recursos de la versión 2 y la versión 3 no permite una actualización sin interrupciones. Puede seguir utilizando la versión 2 para conservar la configuración de asignación de ancho de banda para las máquinas virtuales o puede cambiar a la versión 3 y adaptar una directiva de ancho de banda para los hosts del conmutador.

Tabla 11-1. Versión de Network I/O Control según la versión de vSphere Distributed Switch y ESXi

vSphere Network I/O Control	Versión de vSphere Distributed Switch	Versión de ESXi
2.0	5.1.0	■ 5.1 ■ 5.5 ■ 6.0
	5.5.0	■ 5.5 ■ 6.0
3.0	6.0.0	6.0

Disponibilidad de características

SR-IOV no está disponible para las máquinas virtuales configuradas para utilizar Network I/O Control versión 3.

Actualizar Network I/O Control a la versión 3 en vSphere Distributed Switch

Si actualizó vSphere Distributed Switch a la versión 6.0.0 sin convertir Network I/O Control a la versión 3, puede actualizar Network I/O Control para utilizar el modelo mejorado de asignación de ancho de banda al tráfico del sistema y a máquinas virtuales individuales.

Al actualizar Network I/O Control de la versión 2 a la versión 3, la configuración de todos los grupos de recursos de red del sistema definidos en la versión 2 se convierten en construcciones de recursos compartidos, reservas y límites para el tráfico del sistema. Las reservas de todos los tipos de tráfico del sistema convertidos no se establecen de forma predeterminada.

La actualización de un conmutador distribuido a la versión 3 es disruptiva. Algunas funcionalidades están disponibles únicamente en la versión 2 de Network I/O Control y se quitan con la actualización a la versión 3.

Tabla 11-2. Funcionalidad que se quita durante la actualización a Network I/O Control versión 3

Funcionalidad que se quita durante la actualización	Descripción
Recursos de red definidos por el usuario, incluidas las asociaciones entre ellos y los grupos de puertos distribuidos existentes	Puede conservar ciertas opciones de configuración de la asignación de recursos si transfiere los recursos compartidos de los grupos de recursos de red definidos por el usuario a recursos de red de adaptadores de red individuales. Por lo tanto, antes de actualizar a Network I/O Control versión 3, tome las medidas necesarias para reducir el impacto de la actualización en la asignación de ancho de banda configurada para las máquinas virtuales en Network I/O Control versión 2.
Asociaciones existentes entre los puertos y los grupos de recursos de red definidos por el usuario	En Network I/O Control versión 3, no puede asociar un puerto distribuido individual a un grupo de recursos de red diferente del grupo asignado al grupo de puertos primario. A diferencia de la versión 2, Network I/O Control versión 3 no permite anular la directiva de asignación de recursos para puertos individuales.
Etiquetado de CoS del tráfico asociado con un grupo de recursos de red	Network I/O Control versión 3 no admite que el tráfico que tiene exigencias de QoS superiores se marque con etiquetas de CoS. Después de la actualización, para restaurar el etiquetado de CoS del tráfico asociado con un grupo de recursos de red definido por el usuario, utilice la directiva de redes de filtrado y marcado de tráfico. Consulte Marcar tráfico en un grupo de puertos distribuidos o un grupo de puertos de vínculo superior y Marcar tráfico en un puerto distribuido o un puerto de vínculo superior.

Requisitos previos

- Compruebe que la versión de vSphere Distributed Switch sea 6.0.0.
- Compruebe que la característica Network I/O Control del conmutador distribuido sea de la versión 2.
- Compruebe que tenga el privilegio **Grupo dvPort.Modificar** en los grupos de puertos distribuidos del conmutador.
- Compruebe que todos los hosts del conmutador estén conectados a vCenter Server.

Procedimiento

1. En vSphere Web Client, desplácese hasta el conmutador distribuido.
2. En el menú **Acciones**, seleccione **Actualización > Actualizar Network I/O Control**.

   Aparece el asistente **Actualizar Network I/O Control**.
3. (opcional) En la página Descripción general, cree una copia de seguridad de la configuración del conmutador.

   Puede utilizar esta copia de seguridad para restaurar la configuración del conmutador si hubiera errores en la actualización.

4 Revise los cambios incorporados por la actualización y haga clic en **Siguiente**.

5 Compruebe que el conmutador distribuido cumpla los requisitos previos de validación para la actualización y haga clic en **Siguiente**.

Requisitos previos	Descripción
Accesibilidad al grupo de puertos	Posee privilegios para acceder y modificar el vínculo superior y los grupos de puertos distribuidos en el conmutador.
Estado del host	Todos los hosts del conmutador están conectados a vCenter Server.
Etiquetado de CoS prioritario para el tráfico del sistema	El conmutador distribuido no tiene grupos de recursos de red con etiquetas de CoS asignadas.
Grupos de recursos de red definidos por el usuario	El conmutador distribuido no contiene grupos de recursos definidos por el usuario para control del ancho de banda de máquina virtual.
Anulación de directiva de asignación de recursos	No hay grupos de puertos distribuidos en el conmutador que permitan anular la directiva de Network I/O Control en puertos individuales.

6 Si el conmutador distribuido contiene grupos de recursos definidos por el usuario, transfiera los recursos compartidos de los grupos de recursos definidos por el usuario en la versión 2 a recursos compartidos de los adaptadores de red de máquina virtual individuales en la versión 3 y, a continuación, haga clic en **Siguiente**.

   Transferir los recursos compartidos permite conservar ciertas opciones de configuración de asignación de ancho de banda de las máquinas virtuales.

   Nota Los límites de los grupos de recursos de red definidos por el usuario no se conservan durante la conversión.

7 Revise la configuración de la actualización y haga clic en **Finalizar**.

Pasos siguientes

- Para asignar una cuota de ancho de banda de reserva a un grupo de máquinas virtuales conectadas al conmutador, cree grupos de recursos de red y asócielos con los grupos de puertos distribuidos a los cuales están asociadas las máquinas virtuales. Consulte Crear un grupo de recursos de red y Agregar un grupo de puertos distribuidos a un grupo de recursos de red.

  Si transfirió los recursos compartidos originales desde la versión 2, se aplicarán cuando asocie los grupos de recursos de red con los grupos de puertos del conmutador.

- Para asignar ancho de banda de la cuota a máquinas virtuales individuales, use los recursos compartidos, las reservas y los límites. Consulte Configurar la asignación de ancho de banda para una máquina virtual.

Habilitar Network I/O Control en vSphere Distributed Switch

Habilite la administración de recursos de red en vSphere Distributed Switch para garantizar el ancho de banda mínimo para el tráfico de sistema de las características de vSphere y el tráfico de máquina virtual.

Requisitos previos

Compruebe que la versión de vSphere Distributed Switch sea 5.1.0 o posterior.

Procedimiento

1 En vSphere Web Client, desplácese hasta el conmutador distribuido.

2 En el menú **Acciones**, seleccione **Editar configuración**.

3 En el menú desplegable **Network I/O Control**, seleccione **Habilitar**.

4 Haga clic en **Aceptar**.

Resultados

Cuando Network I/O Control está habilitado, el modelo que usa para manejar la asignación de ancho de banda para el tráfico de sistema y el tráfico de máquina virtual depende de la versión de Network I/O Control activa en el conmutador distribuido. Consulte Acerca de vSphere Network I/O Control versión 3.

Asignar ancho de banda para el sistema de tráfico

Puede configurar Network I/O Control para asignar cierta cantidad de ancho de banda al tráfico generado por vSphere Fault Tolerance, vSphere vMotion, etc.

Puede utilizar Network I/O Control en un conmutador distribuido para configurar la asignación de ancho de banda correspondiente al tráfico que se relaciona con las principales características de vSphere:

- Administración
- Fault Tolerance
- NFS
- vSAN
- vMotion
- vSphere Replication
- Copia de seguridad de vSphere Data Protection
- Máquina virtual

vCenter Server propaga la asignación desde el conmutador distribuido hasta cada adaptador físico en los hosts que están conectados al conmutador.

- Parámetros de asignación de ancho de banda para el tráfico del sistema

  Mediante varios parámetros de configuración, Network I/O Control asigna el ancho de banda al tráfico de las características básicas del sistema vSphere.

- Ejemplo de reserva de ancho de banda para el tráfico del sistema

  La capacidad de los adaptadores físicos determina el ancho de banda garantizado. De acuerdo con esta capacidad, se puede garantizar un ancho de banda mínimo para una característica del sistema de manera que su funcionamiento sea óptimo.

- Configurar la asignación de ancho de banda para el tráfico del sistema

  Asigne el ancho de banda para la administración de hosts, las máquinas virtuales, el almacenamiento NFS, vSphere vMotion, vSphere Fault Tolerance, vSAN y vSphere Replication en los adaptadores físicos conectados a vSphere Distributed Switch.

Parámetros de asignación de ancho de banda para el tráfico del sistema

Mediante varios parámetros de configuración, Network I/O Control asigna el ancho de banda al tráfico de las características básicas del sistema vSphere.

Tabla 11-3. Parámetros de asignación de tráfico de sistema

Parámetro de asignación de ancho de banda	Descripción
Recursos compartidos	Los recursos compartidos, de 1 a 100, reflejan la prioridad relativa de un tipo de tráfico de sistema con respecto a los demás tipos de tráfico de sistema activos en el mismo adaptador físico. La cantidad de ancho de banda disponible para un tipo de tráfico de sistema se determina en función de sus recursos compartidos relativos y la cantidad de datos que transmiten las demás características del sistema.
Reserva	El ancho de banda mínimo, en Mbps, que se debe garantizar en un adaptador físico. El total de ancho de banda reservado entre todos los tipos de tráfico de sistema no puede superar el 75 % del ancho de banda que puede proporcionar el adaptador de red físico de menor capacidad. El ancho de banda reservado que no se usa queda disponible para los demás tipos de tráfico de sistema. Sin embargo, Network I/O Control no redistribuye la capacidad no usada por el tráfico de sistema para la selección de máquinas virtuales.
Límite	El ancho de banda máximo, en Mbps o Gbps, que puede consumir un tipo de tráfico de sistema en un adaptador físico.

Ejemplo de reserva de ancho de banda para el tráfico del sistema

La capacidad de los adaptadores físicos determina el ancho de banda garantizado. De acuerdo con esta capacidad, se puede garantizar un ancho de banda mínimo para una característica del sistema de manera que su funcionamiento sea óptimo.

Por ejemplo, en un conmutador distribuido que está conectado a hosts ESXi con adaptadores de red de 10 GbE, se puede configurar la reserva a fin de garantizar 1 Gbps para la administración mediante vCenter Server, 1 Gbps para vSphere Fault Tolerance, 1 Gbps para el tráfico de vSphere vMotion y 0,5 Gbps para el tráfico de la máquina virtual. Network I/O Control asigna el ancho de banda solicitado en cada adaptador físico de red. Se puede reservar hasta un 75 % del ancho de banda de un adaptador físico de red, es decir, no más de 7,5 Gbps.

Se puede dejar más capacidad sin reservar para que el host asigne ancho de banda de forma dinámica de acuerdo con los recursos compartidos, los límites y el uso, y para reservar únicamente el ancho de banda suficiente para el funcionamiento de una característica del sistema.

Configurar la asignación de ancho de banda para el tráfico del sistema

Asigne el ancho de banda para la administración de hosts, las máquinas virtuales, el almacenamiento NFS, vSphere vMotion, vSphere Fault Tolerance, vSAN y vSphere Replication en los adaptadores físicos conectados a vSphere Distributed Switch.

Para habilitar la asignación de ancho de banda para máquinas virtuales a través de Network I/O Control, configure el tráfico del sistema de la máquina virtual. La reserva de ancho de banda para el tráfico de máquina virtual también se usa para el control de admisión. Cuando se enciende una máquina virtual, el control de admisión verifica que haya suficiente ancho de banda.

Requisitos previos

- Compruebe que la versión de vSphere Distributed Switch sea 6.0.0 o posterior.
- Compruebe que la versión de Network I/O Control en el conmutador sea 3.
- Compruebe que Network I/O Control esté habilitado. Consulte Habilitar Network I/O Control en vSphere Distributed Switch.

Procedimiento

1. En vSphere Web Client, desplácese hasta el conmutador distribuido.
2. En la pestaña **Configurar**, expanda **Asignación de recursos**.
3. Haga clic en **Tráfico del sistema**.

   Puede ver la asignación de ancho de banda para los tipos de tráfico del sistema.
4. Seleccione el tipo de tráfico de acuerdo con la característica vSphere que desee aprovisionar y haga clic en **Editar**.

   Se muestra la configuración de recursos de red para el tipo de tráfico.

5 En el menú desplegable **Recursos compartidos**, modifique la proporción de tráfico que corresponde al flujo general que pasa por un adaptador físico.

   Cuando se satura un adaptador físico, Network I/O Control aplica los recursos compartidos.

   Se puede seleccionar una opción para establecer un valor predefinido o se puede seleccionar **Personalizado** y escribir un número de 1 a 100 para establecer otro recurso compartido.

6 En el cuadro de texto **Reserva**, introduzca un valor para el ancho de banda mínimo que debe estar disponible para el tipo de tráfico.

   La reserva total para el tráfico del sistema no debe superar el 75 % del ancho de banda admitido por el adaptador físico de menor capacidad de todos los adaptadores conectados al conmutador distribuido.

7 En el cuadro de texto **Límite**, establezca el ancho de banda máximo que puede utilizar el tráfico del sistema del tipo seleccionado.

8 Haga clic en **Aceptar** para aplicar la configuración de asignación.

Resultados

vCenter Server propaga la asignación desde el conmutador distribuido hasta los adaptadores físicos de hosts que están conectados al conmutador.

Asignar ancho de banda para el tráfico de la máquina virtual

La versión 3 de Network I/O Control permite configurar los requisitos de ancho de banda de las máquinas virtuales individuales. También puede utilizar grupos de recursos de red en los que podrá asignar una cuota de ancho de banda desde la reserva agregada para el tráfico de la máquina virtual y, a continuación, asignar ancho de banda desde el grupo hasta las máquinas virtuales individuales.

Acerca de la asignación de ancho de banda para máquinas virtuales

Network I/O Control asigna ancho de banda para máquinas virtuales según dos modelos: asignación para todo vSphere Distributed Switch de acuerdo con los grupos de recursos de red y asignación en el adaptador físico que transmite el tráfico de una máquina virtual.

Grupos de recursos de red

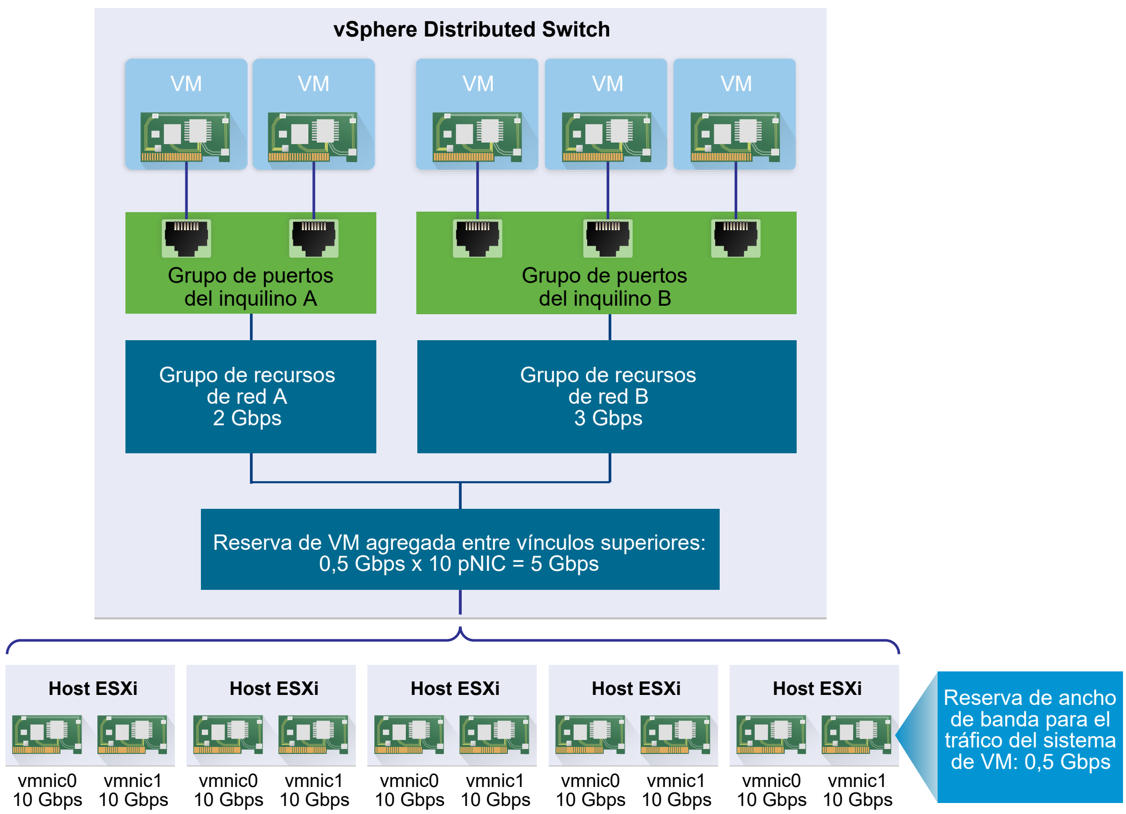
Un grupo de recursos de red representa un fragmento del ancho de banda combinado que se reserva para el tráfico del sistema de máquina virtual en todos los adaptadores físicos conectados al conmutador distribuido.

Por ejemplo, si el tráfico del sistema de máquina virtual tiene 0,5 Gbps reservados en cada vínculo superior de 10 GbE en un conmutador distribuido con 10 vínculos superiores, el ancho de banda combinado total para la reserva de máquina virtual en este conmutador es de 5 Gbps. Cada grupo de recursos de red puede reservar una cuota de estos 5 Gbps de capacidad.

La cuota de ancho de banda asignada exclusivamente a un grupo de recursos de red se comparte entre los grupos de puertos distribuidos asociados con el grupo. Una máquina virtual recibe ancho de banda del grupo a través del grupo de puertos distribuidos al cual está conectada la máquina virtual.

De forma predeterminada, los grupos de puertos distribuidos del conmutador se asignan a un grupo de recursos de red predeterminado cuya cuota no se puede configurar.

Figura 11-1. Sumar ancho de banda para grupos de recursos de red entre los vínculos superiores de vSphere Distributed Switch



Definir los requisitos de ancho de banda para una máquina virtual

Para asignar ancho de banda a una máquina virtual individual, se usa un proceso similar a la asignación de recursos de CPU y de memoria. Network I/O Control versión 3 aprovisiona ancho de banda a una máquina virtual de acuerdo con los recursos compartidos, las reservas y los límites que se definen para un adaptador de red en la configuración de hardware de la máquina virtual. La reserva representa una garantía de que el tráfico de la máquina virtual puede consumir al menos la cantidad de ancho de banda especificada. Si un adaptador físico tiene más capacidad, la máquina virtual puede usar un ancho de banda adicional según los recursos compartidos y los límites especificados.

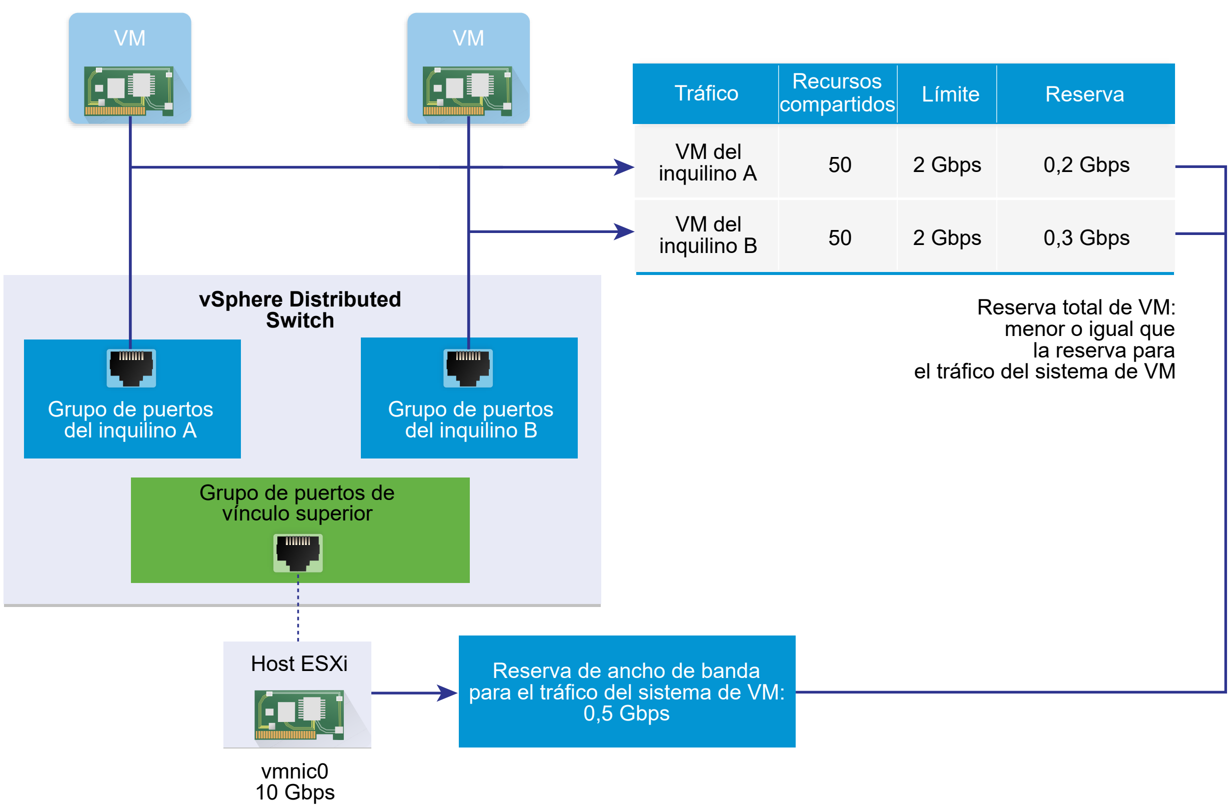
Aprovisionar ancho de banda a una máquina virtual en el host

Para garantizar el ancho de banda, Network I/O Control implementa un motor de selección de tráfico que se activa cuando una máquina virtual tiene configurada la reserva de ancho de banda. Este conmutador distribuido intenta enviar el tráfico de un adaptador de red de máquina virtual al adaptador físico que pueda suministrar el ancho de banda necesario y se encuentre dentro de la directiva de formación de equipos activa.

La reserva de ancho de banda total de las máquinas virtuales en un host no puede superar el ancho de banda reservado que se configuró para el tráfico del sistema de máquina virtual.

El límite y la reserva reales también dependen de la directiva de catalogación de tráfico del grupo de puertos distribuidos al cual está conectado el adaptador. Por ejemplo, si un adaptador de máquina virtual requiere un límite de 200 Mbps, y el ancho de banda promedio configurado en la directiva de catalogación de tráfico es de 100 Mbps, el límite efectivo es de 100 Mbps.

Figura 11-2. Configuración de la asignación de ancho de banda para máquinas virtuales individuales



Tráfico	Recursos compartidos	Límite	Reserva
VM del inquilino A	50	2 Gbps	0,2 Gbps
VM del inquilino B	50	2 Gbps	0,3 Gbps

Parámetros de asignación de ancho de banda para el tráfico de máquinas virtuales

Network I/O Control versión 3 asigna ancho de banda a máquinas virtuales individuales en función de los recursos compartidos, la reserva y los límites configurados para los adaptadores de red en las opciones de hardware de máquina virtual.

Tabla 11-4. Parámetros de asignación de ancho de banda para un adaptador de red de máquina virtual

Parámetro de asignación de ancho de banda	Descripción
Cuota	La prioridad relativa, de 1 a 100, del tráfico que pasa por este adaptador de red de máquina virtual respecto de la capacidad del adaptador físico que transporta el tráfico de máquina virtual hacia la red.
Reserva	El ancho de banda mínimo, en Mbps, que debe recibir el adaptador de red de máquina virtual en el adaptador físico.
Límite	El ancho de banda máximo en el adaptador de red de máquina virtual para el tráfico hacia otras máquinas virtuales en el mismo host o en uno diferente.

Control de admisión del ancho de banda de máquina virtual

Para garantizar la disponibilidad de un ancho de banda suficiente para una máquina virtual, vSphere implementa el control de admisión en el host y en el clúster según se establece en la directiva de reserva de ancho de banda y formación de equipos.

Control de admisión de ancho de banda en vSphere Distributed Switch

Cuando se enciende una máquina virtual, la característica Network I/O Control de un conmutador distribuido comprueba que estas condiciones se cumplan en el host.

- Un adaptador físico del host puede suministrar el ancho de banda mínimo a los adaptadores de red de máquina virtual según la directiva de formación de equipos y reserva.
- La reserva de un adaptador de red de máquina virtual es menor que la cuota libre en el grupo de recursos de red.

Si modifica la reserva de un adaptador de red de una máquina virtual en ejecución, Network I/O Control comprueba nuevamente si el grupo de recursos de red asociado puede admitir la nueva reserva. Si el grupo no tiene una cuota sin uso suficiente, no se aplica el cambio.

Para usar el control de admisión en vSphere Distributed Switch, ejecute las siguientes tareas:

- Configure la asignación de ancho de banda para el tráfico del sistema de máquina virtual en el conmutador distribuido.
- Configure un grupo de recursos de red con una cuota de reserva del ancho de banda configurado para el tráfico del sistema de máquina virtual.
- Asocie el grupo de recursos de red con el grupo de puertos distribuidos que conecta las máquinas virtuales al conmutador.
- Configure los requisitos de ancho de banda de una máquina virtual conectada al grupo de puertos.

Control de admisión de ancho de banda en vSphere DRS

Si enciende una máquina virtual que corresponde a un clúster, vSphere DRS asigna la máquina virtual de un host con la capacidad para garantizar el ancho de banda reservado para la máquina virtual en función de la directiva de formación de equipos activa.

vSphere DRS migra una máquina virtual a otro host para satisfacer la reserva de ancho de banda de la máquina virtual en estas situaciones:

- La reserva se cambia por un valor que el host inicial ya no puede satisfacer.
- Un adaptador físico que transmite tráfico desde la máquina virtual no tiene conexión.

Para usar el control de admisión en vSphere DRS, ejecute las siguientes tareas:

- Configure la asignación de ancho de banda para el tráfico del sistema de máquina virtual en el conmutador distribuido.
- Configure los requisitos de ancho de banda de una máquina virtual conectada al conmutador distribuido.

Para obtener más información sobre la administración de recursos según las demandas de ancho de banda de las máquinas virtuales, consulte la documentación de *Administrar recursos de vSphere*.

Control de admisión de ancho de banda en vSphere HA

Cuando un host falla o queda aislado, vSphere HA enciende una máquina virtual de otro host en el clúster de acuerdo con la directiva de reserva de ancho de banda y formación de equipos.

Para usar el control de admisión en vSphere HA, ejecute las siguientes tareas:

- Asigne ancho de banda para el tráfico del sistema de máquina virtual.
- Configure los requisitos de ancho de banda de una máquina virtual conectada al conmutador distribuido.

Para obtener más información sobre cómo vSphere HA brinda conmutación por error según las demandas de ancho de banda de las máquinas virtuales, consulte la documentación de *Disponibilidad de vSphere*.

Crear un grupo de recursos de red

Cree grupos de recursos de red en vSphere Distributed Switch para reservar el ancho de banda de un conjunto de máquinas virtuales.

Un grupo de recursos de red proporciona una cuota de reserva para las máquinas virtuales. La cuota representa una parte del ancho de banda que se reserva para el tráfico de sistema de la máquina virtual en los adaptadores físicos conectados al conmutador distribuido. Se puede separar una parte de ancho de banda de la cuota para las máquinas virtuales que están asociadas al grupo. La reserva de los adaptadores de red de las máquinas virtuales encendidas que están asociadas al grupo no debe superar la cuota del grupo. Consulte Acerca de la asignación de ancho de banda para máquinas virtuales.

Requisitos previos

- Compruebe que la versión de vSphere Distributed Switch sea 6.0.0 o posterior.
- Compruebe que la versión de Network I/O Control en el conmutador sea 3.
- Compruebe que Network I/O Control esté habilitado. Consulte Habilitar Network I/O Control en vSphere Distributed Switch.
- Compruebe que se haya configurado una reserva de ancho de banda para el tráfico de sistema de máquina virtual. Consulte Configurar la asignación de ancho de banda para el tráfico del sistema.

Procedimiento

1. En vSphere Web Client, desplácese hasta el conmutador distribuido.
2. En la pestaña **Configurar**, expanda **Asignación de recursos**.
3. Haga clic en **Grupos de recursos de red**.
4. Haga clic en el icono **Agregar**.
5. (opcional) Introduzca un nombre y una descripción para el grupo de recursos de red.
6. Introduzca un valor en Mbps para **Cuota de reserva** a partir del ancho de banda libre reservado para el tráfico de sistema de la máquina virtual.

   La cuota máxima que es posible asignar al grupo se determina en función de la siguiente fórmula:

   ```
   max reservation quota = aggregated reservation for vm system traffic - quotas of the other
   resource pools
   ```

   donde

   - `aggregated reservation for vm system traffic` = reserva de ancho de banda configurada para el tráfico de sistema de la máquina virtual en cada pNIC * la cantidad de pNIC conectadas al conmutador distribuido
   - `quotas of the other pools` = suma de las cuotas de reserva de los otros grupos de recursos de red
7. Haga clic en **Aceptar**.

Pasos siguientes

Agregue uno o más grupos de puertos distribuidos al grupo de recursos de red de modo que pueda asignar ancho de banda a las máquinas virtuales individuales a partir de la cuota del grupo. Consulte Agregar un grupo de puertos distribuidos a un grupo de recursos de red.

Agregar un grupo de puertos distribuidos a un grupo de recursos de red

Agregue un grupo de puertos distribuidos a un grupo de recursos de red para poder asignar ancho de banda a las máquinas virtuales conectadas al grupo de puertos.

Para asignar un grupo de recursos de red a varios grupos de puertos distribuidos al mismo tiempo, puede utilizar la directiva de asignación de recursos del asistente **Administrar grupos de puertos distribuidos**. Consulte Administrar directivas para varios grupos de puertos en vSphere Distributed Switch.

Network I/O Control asigna ancho de banda a las máquinas virtuales asociadas con el grupo de puertos distribuidos en función del modelo implementado en la versión Network I/O Control activa en el conmutador distribuido. Consulte Acerca de vSphere Network I/O Control versión 3.

Requisitos previos

- Compruebe que la versión de vSphere Distributed Switch sea 5.1 o posterior.
- Compruebe que Network I/O Control esté habilitado. Consulte Habilitar Network I/O Control en vSphere Distributed Switch.

Procedimiento

1 Busque un grupo de puertos distribuidos en vSphere Web Client.

   a Seleccione un conmutador distribuido y haga clic en la pestaña **Redes**.

   b Haga clic en **Grupos de puertos distribuidos**.

2 Seleccione el grupo de puertos distribuidos y haga clic en **Editar configuración de grupo de puertos distribuidos**.

3 En el cuadro de diálogo Editar configuración, haga clic en **General**.

4 En el menú desplegable **Grupo de recursos de red**, seleccione el grupo de recursos de red y haga clic en **Aceptar**.

   Si el conmutador distribuido no contiene grupos de recursos de red, solamente se muestra la opción **(predeterminado)** en el menú desplegable.

Configurar la asignación de ancho de banda para una máquina virtual

Es posible configurar la asignación del ancho de banda a las máquinas virtuales individuales que están conectadas a un grupo de puertos distribuidos. Se puede utilizar la configuración de recursos compartidos, reserva y límite para el ancho de banda.

Requisitos previos

- Compruebe que la versión de vSphere Distributed Switch sea 6.0.0 o posterior.
- Compruebe que la versión de Network I/O Control en el conmutador sea 3.

- Compruebe que Network I/O Control esté habilitado. Consulte Habilitar Network I/O Control en vSphere Distributed Switch.
- Compruebe que se haya configurado una reserva de ancho de banda para el tráfico de sistema de máquina virtual. Consulte Configurar la asignación de ancho de banda para el tráfico del sistema.

Procedimiento

1 Ubique la máquina virtual en vSphere Web Client.

   a Seleccione un centro de datos, una carpeta, un clúster, un grupo de recursos o un host y haga clic en la pestaña **Máquinas virtuales**.

   b Haga clic en **Máquinas virtuales** y haga doble clic en la máquina virtual en la lista.

2 En la pestaña **Configurar** de la máquina virtual, expanda **Configuración** y seleccione **Hardware de máquina virtual**.

3 Haga clic en **Editar**.

4 Expanda la sección Network adapter *Adaptador de red X* en el adaptador de red de máquina virtual.

5 Si desea configurar la asignación de ancho de banda de un nuevo adaptador de red de máquina virtual, en el menú desplegable **Dispositivo nuevo** seleccione **Red** y haga clic en **Agregar**.

   La sección Red nueva muestra opciones para la asignación del ancho de banda y otras opciones del adaptador de red.

6 Si el adaptador de red de máquina virtual no está conectado al grupo de puertos distribuidos, seleccione el grupo de puertos en el menú desplegable junto a la etiqueta Network adapter *Adaptador de red X* o Red nueva.

   Se muestra la configuración **Recursos compartidos**, **Reserva** y **Límite** para el adaptador de red de máquina virtual.

7 En el menú desplegable **Recursos compartidos**, establezca la prioridad relativa para el tráfico de esta máquina virtual como recursos compartidos de la capacidad del adaptador físico conectado.

   Cuando se satura un adaptador físico, Network I/O Control aplica los recursos compartidos.

   Se puede seleccionar una opción para establecer un valor predefinido o se puede seleccionar **Personalizado** y escribir un número de 1 a 100 para establecer otro recurso compartido.

8 En el cuadro de texto **Reserva**, reserve el ancho de banda mínimo que debe estar disponible para el adaptador de red de máquina virtual cuando se enciende la máquina virtual.

   Si se aprovisiona ancho de banda mediante un grupo de recursos de red, la reserva de los adaptadores de red de las máquinas virtuales encendidas que se asocian con el grupo no debe exceder la cuota del grupo.

Si vSphere DRS está habilitado, para encender la máquina virtual, asegúrese de que la reserva de todos los adaptadores de red de máquina virtual en el host no supere el ancho de banda reservado para el tráfico de sistema de máquina virtual en los adaptadores físicos de host.

9 En el cuadro de texto **Límite**, establezca un límite para el ancho de banda que pueda consumir el adaptador de red de máquina virtual.

10 Haga clic en **Aceptar**.

Resultados

Red

I/O Control asigna el ancho de banda reservado para el adaptador de red de la máquina virtual desde la cuota de reserva del grupo de recursos de red.

Configurar la asignación de ancho de banda en varias máquinas virtuales

Con una sola operación, puede configurar la asignación de ancho de banda de varias máquinas virtuales conectadas a un grupo de recursos de red específico, por ejemplo, después de actualizar Network I/O Control a la versión 3.

Requisitos previos

- Compruebe que la versión de vSphere Distributed Switch sea 6.0.0 o posterior.
- Compruebe que la versión de Network I/O Control en el conmutador sea 3.
- Compruebe que Network I/O Control esté habilitado. Consulte Habilitar Network I/O Control en vSphere Distributed Switch.
- Compruebe que se haya configurado una reserva de ancho de banda para el tráfico de sistema de máquina virtual. Consulte Configurar la asignación de ancho de banda para el tráfico del sistema.
- Compruebe que las máquinas virtuales estén asociadas con un grupo de recursos de red específico a través de los grupos de puertos distribuidos conectados. Consulte Agregar un grupo de puertos distribuidos a un grupo de recursos de red.

Procedimiento

1 En vSphere Web Client, desplácese hasta el conmutador distribuido.

2 En la pestaña **Configurar**, expanda **Asignación de recursos**.

3 Haga clic en **Grupos de recursos de red**.

4 Seleccione un grupo de recursos de red.

5 Haga clic en **Máquinas virtuales**.

Se muestra una lista de los adaptadores de red de máquina virtual conectados al grupo de recursos de red seleccionado.

6 Seleccione los adaptadores de red de máquina virtual cuyas opciones desee configurar y haga clic en **Editar**.

7 En el menú desplegable **Recursos compartidos**, establezca la prioridad relativa para el tráfico proveniente de estas máquinas virtuales respecto de los adaptadores físicos que transportan el tráfico.

   Cuando se satura un adaptador físico, Network I/O Control aplica los recursos compartidos.

8 En el cuadro de texto **Reserva**, reserve el ancho de banda mínimo que debe estar disponible para cada adaptador de red de máquina virtual cuando se encienden las máquinas virtuales.

   Si se aprovisiona ancho de banda mediante un grupo de recursos de red, la reserva de los adaptadores de red de las máquinas virtuales encendidas que se asocian con el grupo no debe exceder la cuota del grupo.

9 En el cuadro de texto **Límite**, establezca un límite para el ancho de banda que pueda consumir cada adaptador de red de máquina virtual.

10 Haga clic en **Aceptar**.

Cambiar cuota de un grupo de recursos de red

Puede modificar la cuota de ancho de banda que es posible reservar para las máquinas virtuales conectadas a un conjunto de grupos de puertos distribuidos.

Requisitos previos

- Compruebe que la versión de vSphere Distributed Switch sea 6.0.0 o posterior.
- Compruebe que la versión de Network I/O Control en el conmutador sea 3.
- Compruebe que Network I/O Control esté habilitado. Consulte Habilitar Network I/O Control en vSphere Distributed Switch.
- Compruebe que se haya configurado una reserva de ancho de banda para el tráfico de sistema de máquina virtual. Consulte Configurar la asignación de ancho de banda para el tráfico del sistema.

Procedimiento

1 En vSphere Web Client, desplácese hasta el conmutador distribuido.

2 En la pestaña **Configurar**, expanda **Asignación de recursos**.

3 Haga clic en **Grupos de recursos de red**.

4 Seleccione un grupo de recursos de red de la lista y haga clic en **Editar**.

5 En el cuadro de texto **Cuota de reserva**, escriba la cuota de ancho de banda para las máquinas virtuales a partir de la combinación del ancho de banda libre reservado para el tráfico del sistema de máquina virtual en todos los adaptadores físicos del conmutador.

6 Haga clic en **Aceptar**.

Quitar un grupo de puertos distribuidos de un grupo de recursos de red

Para dejar de asignar ancho de banda a las máquinas virtuales a partir de la cuota de reserva de un grupo de recursos de red, quite la asociación entre el grupo de puertos al cual están conectadas las máquinas virtuales y el grupo.

Procedimiento

1 Busque un grupo de puertos distribuidos en vSphere Web Client.

   a Seleccione un conmutador distribuido y haga clic en la pestaña **Redes**.

   b Haga clic en **Grupos de puertos distribuidos**.

2 Seleccione el grupo de puertos distribuidos y haga clic en **Editar configuración de grupo de puertos distribuidos**.

3 En el cuadro de diálogo Editar configuración del grupo de puertos, haga clic en **General**.

4 En el menú desplegable **Grupo de recursos de red**, seleccione **(predeterminado)** y haga clic en **Aceptar**.

Resultados

El grupo de puertos distribuidos se asocia con el grupo de recursos de red de máquina virtual predeterminado.

Eliminar un grupo de recursos de red

Elimine un grupo de recursos cuando ya no se lo utilice.

Requisitos previos

Desacople el grupo de recursos de red de todos los grupos de puertos distribuidos asociados. Consulte Quitar un grupo de puertos distribuidos de un grupo de recursos de red.

Procedimiento

1 En vSphere Web Client, desplácese hasta el conmutador distribuido.

2 En la pestaña **Configurar**, expanda **Asignación de recursos**.

3 Haga clic en **Grupos de recursos de red**.

4 Seleccione un grupo de recursos de red y haga clic en **Quitar**.

5 Haga clic en **Sí** para eliminar el grupo de recursos.

Desplazar un adaptador físico fuera del alcance de Network I/O Control

En determinadas condiciones, puede ser necesario excluir adaptadores físicos con baja capacidad del modelo de asignación de ancho de banda de Network I/O Control versión 3.

Por ejemplo, si la asignación de ancho de banda de vSphere Distributed Switch fue configurada para NIC de 10 GbE, probablemente no pueda agregar una NIC de 1 GbE al conmutador porque esta tarjeta no cumple los requisitos de asignación mayores configurados en las NIC de 10 GbE.

Requisitos previos

- Compruebe que el host ejecute ESXi 6.0 o posterior.
- Compruebe que la versión de vSphere Distributed Switch sea 6.0.0 o posterior.
- Compruebe que la versión de Network I/O Control en el conmutador sea 3.

Procedimiento

1 En vSphere Web Client, desplácese hasta el host.

2 En la pestaña**Configurar**, expanda **Sistema** y seleccione **Configuración avanzada del sistema**.

3 Establezca los adaptadores físicos que necesite fuera del alcance de Network I/O Control con el formato de lista separada por comas para el parámetro `Net.IOControlPnicOptOut`.

   Por ejemplo: **`vmnic0,vmnic3`**.

4 Haga clic en **Aceptar** para aplicar los cambios.

Trabajar con Network I/O Control versión 2

En vSphere Distributed Switch 5.x, al igual que en vSphere Distributed Switch actualizado a 6.0 que no cuente con la actualización de Network I/O Control a la versión 3, puede asegurarse de que el tráfico del sistema y las máquinas virtuales reciban el ancho de banda que necesitan para su operación mediante el modelo de grupo de recursos de Network I/O Control versión 2.

Grupos de recursos de red en Network I/O Control versión 2

En Network I/O Control versión 2, el tráfico del conmutador distribuido admite dos tipos de grupos de recursos de red:

- Grupos de recursos de red del sistema. Grupos predefinidos para controlar el ancho de banda de red que se suministra a los principales tipos de tráfico del sistema: tráfico de Fault Tolerance, tráfico de vMotion, tráfico de administración, tráfico de vSphere Replication, tráfico de NFS y tráfico de máquina virtual.
- Grupos de recursos de red definidos por el usuario. Grupos personalizados para el tráfico de máquinas virtuales. La configuración de un grupo de recursos definido por el usuario se aplica a las máquinas virtuales después de asociar un grupo de recursos definido por el usuario con un grupo de puertos distribuidos.

Parámetros de asignación de ancho de banda para los grupos de recursos de red en Network I/O Control versión 2

Parámetro de asignación de ancho de banda	Descripción
Recursos compartidos	Cuando un adaptador físico está saturado, las máquinas virtuales o los adaptadores VMkernel que utilizan el adaptador reciben ancho de banda para la red externa en función de los recursos compartidos configurados en el grupo de recursos de red. Los recursos compartidos del adaptador físico que se asignan a un grupo de recursos de red determinan la proporción del ancho de banda total disponible que se garantiza para el tráfico asociado con el grupo de recursos de red. La proporción real de ancho de banda del tráfico saliente que está disponible para un grupo de recursos de red se determina en función de los recursos compartidos del grupo de recursos de red, así como en función de los demás grupos de recursos de red con transmisiones activas.
Límite	El límite de hosts de un grupo de recursos de red es el ancho de banda máximo que puede consumir el tráfico asociado con el grupo de recursos de red en un adaptador físico.
Etiqueta de QoS	Asignar una etiqueta de prioridad de QoS a un grupo de recursos de red aplica una etiqueta 802.1p (CoS) a todos los paquetes salientes asociados con el grupo de recursos de red. De esta forma, es posible marcar cierto tráfico para que los dispositivos de red, como los conmutadores, le den mayor prioridad.

Crear un grupo de recursos de red en la versión 2 de Network I/O Control

Cree grupos de recursos de red definidos por el usuario para personalizar la asignación de ancho de banda cuando el tráfico que fluye a través de un adaptador de red físico se vuelve intensivo.

Requisitos previos

- Compruebe que la versión de vSphere Distributed Switch sea 5.1 o posterior.
- Compruebe que la versión de Network I/O Control en el conmutador distribuido sea 2.
- Habilite Network I/O Control en el conmutador distribuido. Consulte Habilitar Network I/O Control en vSphere Distributed Switch.

Procedimiento

1. En vSphere Web Client, desplácese hasta el conmutador distribuido.
2. En la pestaña **Configurar**, expanda **Asignación de recursos**.
3. Haga clic en **Nueva**.
4. Introduzca un nombre y, si desea, una descripción para el grupo de recursos de red.
5. En el cuadro de texto **Límite**, introduzca el límite de ancho de banda (en Mbps) para el grupo de recursos de red con respecto a los adaptadores físicos conectados en el host.

   De forma predeterminada, no se aplica ningún límite sobre el tráfico.

6 En el menú desplegable **Recursos compartidos de adaptador físico**, introduzca los recursos compartidos de la capacidad de adaptador físico que tienen las máquinas virtuales o los adaptadores VMkernel asociados con el grupo de recursos de red.

   Cuando se satura el adaptador físico conectado, Network I/O Control aplica los recursos compartidos configurados.

   Se puede seleccionar una opción para establecer un valor predefinido o se puede seleccionar **Personalizado** e introducir un número de 1 a 100 para establecer otro recurso compartido.

7 (opcional) En el menú desplegable **Etiqueta de prioridad de clase de servicio**, seleccione la etiqueta QoS para marcar el tráfico de sistema o de máquina virtual asociado con el grupo de recursos de red, y haga clic en **Aceptar**.

   La etiqueta de prioridad QoS representa una etiqueta IEEE 802.1p (CoS) para definir la prioridad de tráfico entre las máquinas virtuales asociadas con el grupo de recursos en la Capa 2 de la pila de protocolos de red.

Pasos siguientes

Asocie uno o más grupos de puertos distribuidos con el grupo de recursos de red para aplicar la configuración de control de ancho de banda en las máquinas virtuales. Consulte Agregar un grupo de puertos distribuidos a un grupo de recursos de red.

Editar la configuración de un grupo de recursos de red en la versión 2 de Network I/O Control

Edite la configuración de un sistema o de un grupo de recursos de red definidos por el usuario para cambiar la prioridad del tráfico que se asocia con el grupo en la versión 2 de Network I/O Control.

Requisitos previos

- Compruebe que la versión de vSphere Distributed Switch sea 5.1 o posterior.
- Compruebe que la versión de Network I/O Control en el conmutador distribuido sea 2.
- Habilite Network I/O Control en el conmutador distribuido. Consulte Habilitar Network I/O Control en vSphere Distributed Switch.

Procedimiento

1 En vSphere Web Client, desplácese hasta el conmutador distribuido.

2 En la pestaña **Configurar**, expanda **Asignación de recursos**.

3 Seleccione un grupo de recursos de red de la lista y haga clic en **Editar**.

4 En el cuadro de texto **Límite**, establezca un límite para el ancho de banda que pueda consumir el adaptador de red de máquina virtual.

5 En el menú desplegable **Recursos compartidos de adaptador físico**, introduzca los recursos compartidos de la capacidad de adaptador físico que tienen las máquinas virtuales o los adaptadores VMkernel asociados con el grupo de recursos de red.

   Cuando se satura el adaptador físico conectado, Network I/O Control aplica los recursos compartidos configurados.

   Se puede seleccionar una opción para establecer un valor predefinido o se puede seleccionar **Personalizado** e introducir un número de 1 a 100 para establecer otro recurso compartido.

6 (opcional) En el menú desplegable **Etiqueta de prioridad de clase de servicio**, seleccione la etiqueta QoS para marcar el tráfico de sistema o de máquina virtual asociado con el grupo de recursos de red, y haga clic en **Aceptar**.

   La etiqueta de prioridad QoS representa una etiqueta IEEE 802.1p (CoS) para definir la prioridad de tráfico entre las máquinas virtuales asociadas con el grupo de recursos en la Capa 2 de la pila de protocolos de red.

Resultados

La versión 2 de Network I/O Control aplica la nueva configuración al control de ancho de banda para VMkernel y los adaptadores de máquinas virtuales en los grupos de puertos distribuidos que están asociados con el grupo de recursos de red.

Administrar direcciones MAC

12

Las direcciones MAC se utilizan en la Capa 2 (capa de vínculo de datos) de la pila del protocolo de red para transmitir tramas a un destinatario. En vSphere, vCenter Server genera direcciones MAC para adaptadores de máquinas virtuales y adaptadores VMkernel; también puede asignar manualmente direcciones.

A cada fabricante de adaptadores de red se le asigna un prefijo único de tres bytes denominado identificador único de organización (OUI), que puede utilizarse para generar direcciones MAC únicas.

VMware admite varios mecanismos de asignación de direcciones, cada uno con un OUI individual:

- Direcciones MAC generadas
  - Asignadas por vCenter Server
  - Asignadas por el host ESXi
- Establecer manualmente direcciones MAC
- Generadas para máquinas virtuales heredadas, pero ya no utilizadas en ESXi

Si vuelve a configurar el adaptador de red de una máquina virtual apagada (por ejemplo, al cambiar el tipo de asignación automática de direcciones MAC o al configurar una dirección MAC estática), vCenter Server resolverá el conflicto de la dirección MAC antes de que se produzca la reconfiguración del adaptador.

Este capítulo incluye los siguientes temas:

Asignar la dirección MAC desde vCenter Server

vSphere 5.1 y versiones posteriores proporciona varios esquemas para la asignación automática de direcciones MAC en vCenter Server. Puede seleccionar el esquema que mejor se adapte a sus requisitos para la duplicación de direcciones MAC, para los requisitos OUI correspondientes a direcciones administradas de forma local o universal, y así sucesivamente.

Los siguientes esquemas de generación de direcciones MAC están disponibles en vCenter Server:

- Asignación de OUI VMware, asignación predeterminada
- Asignación basada en prefijos
- Asignación basada en rangos

Después de que se genera la dirección MAC, ya no cambia a menos que la dirección MAC de la máquina virtual entre en conflicto con la de otra máquina virtual registrada. La dirección MAC se guarda en el archivo de configuración de la máquina virtual.

Nota Si utiliza valores de asignación basados en prefijos o basados en rangos no válidos, se registrará un error en el archivo `vpxd.log`. vCenter Server no asigna direcciones MAC cuando aprovisiona una máquina virtual.

Evitar conflictos de la dirección MAC

La dirección MAC de una máquina virtual apagada no se compara con las direcciones de máquinas virtuales suspendidas o en funcionamiento.

Cuando una máquina virtual se vuelve a encender, podría adquirir una dirección MAC diferente. El cambio puede deberse a un conflicto de direcciones con otra máquina virtual. Aunque esta máquina virtual se apagó, su dirección MAC se asignó a otra máquina virtual que se encendió.

Si vuelve a configurar el adaptador de red de una máquina virtual apagada (por ejemplo, al cambiar el tipo de asignación automática de direcciones MAC o al configurar una dirección MAC estática), vCenter Server resolverá los conflictos de la dirección MAC antes de tenga lugar la reconfiguración del adaptador.

Para obtener información sobre la resolución de conflictos de la dirección MAC, consulte la documentación *Solucionar problemas de vSphere*.

Asignación de OUI de VMware

La asignación del identificador único organizativo (OUI) de VMware asigna direcciones MAC basadas en el OUI de VMware predeterminado `00:50:56` y el identificador de vCenter Server.

La asignación de OUI de VMware es el modelo predeterminado de asignación de direcciones MAC para máquinas virtuales. La asignación funciona con hasta 64 instancias de vCenter Server, y cada vCenter Server puede asignar hasta 64.000 direcciones MAC únicas. El esquema de asignación de OUI de VMware es adecuado para implementaciones a pequeña escala.

Formato de dirección MAC

De acuerdo con el esquema de asignación de OUI de VMware, una dirección MAC tiene el formato `00:50:56:`*`XX`*`:`*`YY`*`:`*`ZZ`*, donde `00:50:56` representa el OUI de VMware, *XX* se calcula como (80 + identificador de vCenter Server), e *YY* y *ZZ* son números aleatorios hexadecimales de dos dígitos.

Las direcciones creadas a través de la asignación del OUI de VMware están en el rango de `00:50:56:80:YY:ZZ` - `00:50:56:BF:YY:ZZ`.

Asignar direcciones MAC basada en prefijos

En los hosts ESXi 5.1 y versiones posteriores, puede utilizar la asignación basada en prefijos para especificar un OUI diferente al valor `00:50:56` predeterminado por VMware, o bien introducir direcciones MAC de administración local (LAA) para un espacio de direcciones más amplio.

La asignación de direcciones MAC basada en prefijos supera los límites de la asignación de VMware predeterminada para suministrar direcciones exclusivas en implementaciones de mayor escala. Introducir el prefijo LAA permite obtener un espacio de direcciones MAC muy grande (2 a la 46 potencia) en lugar de contar con un OUI de dirección universal único que solo permite obtener 16 millones de direcciones MAC.

Compruebe que los prefijos que suministra para las diferentes instancias de vCenter Server en una misma red sean exclusivos. vCenter Server utiliza los prefijos para evitar problemas de duplicación de direcciones MAC. Consulte la documentación de *Solucionar problemas de vSphere*.

Asignar direcciones MAC basada en rangos

En las versiones de host ESXi 5.1 y posteriores, se puede utilizar una asignación basada en rangos para incluir o excluir rangos de direcciones de administración local (LAA).

Es posible especificar uno o más rangos mediante direcciones MAC iniciales y finales, por ejemplo, (`02:50:68:00:00:02`, `02:50:68:00:00:FF`). Las direcciones MAC se generan solamente a partir del rango especificado.

Puede especificar varios rangos de LAA y vCenter Server realiza un seguimiento de la cantidad de direcciones utilizadas para cada rango. vCenter Server asigna direcciones MAC del primer rango que aún tiene direcciones disponibles. vCenter Server comprueba si hay conflictos de direcciones MAC dentro de sus rangos.

Cuando se utiliza la asignación basada en rangos, se deben proporcionar diferentes instancias de vCenter Server con rangos que no se superpongan. vCenter Server no detecta rangos que puedan estar en conflicto con otras instancias de vCenter Server. Consulte la documentación de *Solucionar problemas de vSphere* para obtener más información sobre cómo solucionar problemas con direcciones MAC duplicadas.

Nota La configuración de asignación de direcciones MAC basada en rangos se pierde cuando se actualiza a una nueva versión de vCenter Server. Debe volver a crear manualmente la configuración de asignación de direcciones MAC basada en rangos después de la actualización.

Asignar una dirección MAC

Utilice vSphere Web Client para habilitar la asignación de direcciones MAC basada en prefijos o en rangos y para ajustar los parámetros de asignación.

Si cambia de un tipo de asignación a otro, por ejemplo, de la asignación de OUI de VMware a una asignación basada en rangos, utilice vSphere Web Client. Sin embargo, cuando hay un esquema basado en prefijos o rangos y desea cambiarlo por otro esquema de asignación, debe editar el archivo `vpxd.cfg` manualmente y reiniciar vCenter Server.

Cambiar o ajustar asignaciones basadas en rangos o prefijos

Cambiar el OUI de VMware predeterminado por la asignación de direcciones MAC basada en rangos o prefijos a través de vSphere Web Client permite evitar y resolver conflictos de duplicación de direcciones MAC en las implementaciones de vSphere.

Para cambiar el esquema de asignación del OUI de VMware predeterminado a la asignación basada en rangos o prefijos, use las opciones de **Configuración avanzada** disponibles para la instancia de vCenter Server en vSphere Web Client.

Para cambiar la asignación basada en rangos o prefijos y volver a la asignación de OUI de VMware, o para cambiar entre la asignación basada en rangos y la basada en prefijos, modifique manualmente el archivo `vpxd.cfg`. Consulte Establecer o cambiar el tipo de asignación.

Nota Debe utilizar la asignación de direcciones MAC basada en prefijos en los hosts de vCenter Server 5.1 y ESXi 5.1, y posteriores.

Si una instancia de vCenter Server 5.1 administra hosts que están ejecutando versiones de ESXi anteriores a ESXi 5.1, utilice la asignación de direcciones MAC basada en prefijos del OUI de VMware. Las máquinas virtuales que tengan asignadas direcciones MAC basadas en prefijos del OUI que no sean de VMware no podrán encenderse en los hosts anteriores a la versión 5.1. Estos hosts comprueban de manera explícita si una dirección MAC asignada utiliza el prefijo 00:50:56 del OUI de VMware.

Procedimiento

1 En vSphere Web Client, desplácese hasta una instancia de vCenter Server.

2 En la pestaña **Configurar**, expanda **Configuración** y seleccione **Configuración avanzada**.

3 Haga clic en **Editar**.

4 Agregue o edite los parámetros del tipo de asignación de destino.

   Utilice un solo tipo de asignación.

   - Cambie la asignación basada en prefijos.

Clave	Valor de ejemplo
`config.vpxd.macAllocScheme.prefixScheme.prefix`	005026
`config.vpxd.macAllocScheme.prefixScheme.prefixLength`	23

     `prefix` y `prefixLength` determinan el rango de prefijos de dirección MAC que tienen las vNIC recién agregadas. `prefix` es el OUI inicial de las direcciones MAC relacionadas con la instancia de vCenter Server, mientras que `prefixLength` determina la longitud del prefijo en bits.

Por ejemplo, la configuración de la tabla genera direcciones MAC de la NIC de máquina virtual desde 00:50:26 o 00:50:27.

- Cambie la asignación a una basada en rangos.

Clave	Valor de ejemplo
`config.vpxd.macAllocScheme.rangeScheme.range[X].begin`	005067000000
`config.vpxd.macAllocScheme.rangeScheme.range[X].end`	005067ffffff

X en `range[X]` es el número de secuencia del rango. Por ejemplo, `0` en `range[0]` representa la configuración de la asignación del primer rango de la asignación de direcciones MAC.

5 Haga clic en **Aceptar**.

Establecer o cambiar el tipo de asignación

Si desea cambiar de una asignación basada en prefijos o rangos a una asignación de OUI de VMware, debe establecer el tipo de asignación en el archivo `vpxd.cfd` y reiniciar vCenter Server.

Requisitos previos

Defina el tipo de asignación antes de cambiar el archivo `vpxd.cfg`. Para obtener información sobre los tipos de asignación, consulte Asignar la dirección MAC desde vCenter Server.

Procedimiento

1 En el equipo host de vCenter Server, desplácese hasta el directorio que contiene el archivo de configuración:

- En un sistema operativo Windows Server, la ubicación del directorio es `C:\ProgramData\VMware\CIS\cfg\vmware-vpx`.
- En vCenter Server Appliance, la ubicación del directorio es `/etc/vmware-vpx`.

2 Abra el archivo `vpxd.cfg`.

3 Defina el tipo de asignación que desea utilizar y escriba el código XML correspondiente en el archivo para configurar el tipo de asignación.

A continuación, se muestran ejemplos del código XML que se puede utilizar.

Nota Utilice un solo tipo de asignación.

- Asignación de OUI de VMware

```
<vpxd>
   <macAllocScheme>
      <VMwareOUI>true</VMwareOUI>
   </macAllocScheme>
</vpxd>
```

- Asignación basada en prefijos

```
 <vpxd>
    <macAllocScheme>
      <prefixScheme>
         <prefix>005026</prefix>
         <prefixLength>23</prefixLength>
      </prefixScheme>
   </macAllocScheme>
</vpxd>
```

- Asignación basada en rangos

```
<vpxd>
   <macAllocScheme>
       <rangeScheme>
          <range id="0">
             <begin>005067000001</begin>
             <end>005067000001</end>
          </range>
       </rangeScheme>
   </macAllocScheme>
</vpxd>
```

4 Guarde el archivo `vpxd.cfg`.

5 Reinicie el host de vCenter Server.

Generar direcciones MAC en hosts ESXi

Un host ESXi genera la dirección MAC para un adaptador de la máquina virtual cuando el host no está conectado a vCenter Server. Tales direcciones tienen un identificador de organización único (OUI) de VMware para evitar conflictos.

El host ESXi genera la dirección MAC para un adaptador de la máquina virtual en uno de los siguientes casos:

- El host no está conectado a vCenter Server.

- El archivo de configuración de la máquina virtual no contiene la dirección MAC ni la información sobre el tipo de asignación de direcciones MAC.

Formato de dirección MAC

El host genera direcciones MAC compuestas por el OUI de VMware `00:0C:29` y los últimos tres octetos en formato hexadecimal del identificador universal único (UUID) de la máquina virtual. El UUID de la máquina virtual se basa en un código hash que se calcula mediante el UUID de la máquina física de ESXi y la ruta del archivo de configuración (`.vmx`) de la máquina virtual.

Evitar conflictos de la dirección MAC

Se realiza un seguimiento para detectar conflictos en todas las direcciones MAC que se asignaron a adaptadores de red de las máquinas virtuales en ejecución y suspendidas en una máquina física específica.

Si importa una máquina virtual con una dirección MAC generada por el host de un sistema vCenter Server a otro, seleccione la opción **Lo copié** al encender la máquina virtual para volver a generar la dirección y evitar posibles conflictos en el sistema vCenter Server de destino o entre los sistemas vCenter Server.

Configurar una dirección MAC estática para una máquina virtual

En la mayoría de las implementaciones de red, un buen enfoque son las direcciones MAC generadas. Sin embargo, es posible que se deba establecer una dirección MAC estática para un adaptador de máquina virtual con un valor único.

Los siguientes casos muestran cuándo se podría establecer una dirección MAC estática:

- Los adaptadores de máquinas virtuales en diferentes hosts físicos comparten la misma subred y tienen asignada la misma dirección MAC, lo cual produce un conflicto.
- Asegúrese de que el adaptador de máquina virtual tenga siempre la misma dirección MAC.

VMware utiliza de forma predeterminada el identificador único organizativo (OUI) `00:50:56` para las direcciones generadas manualmente, pero todas las direcciones únicas generadas manualmente son compatibles.

Nota Compruebe que no haya otros dispositivos ajenos a VMware. Para ello, utilice las direcciones asignadas a los componentes de VMware. Por ejemplo, podría haber servidores físicos en la misma subred que utilicen `11:11:11:11:11:11`, `22:22:22:22:22:22` como direcciones MAC estáticas. Los servidores físicos no pertenecen al inventario de vCenter Server, por lo cual vCenter Server no puede comprobar si hay conflictos en las direcciones.

OUI de VMware en direcciones MAC estáticas

De forma predeterminada, las direcciones MAC utilizan el identificador de organización único (OUI) de VMware como prefijo. No obstante, el rango de direcciones libres proporcionado por el OUI de VMware es restringido.

Si decide utilizar el OUI de VMware, parte del rango se reserva para vCenter Server, las NIC físicas del host, las NIC virtuales y para uso futuro.

Puede establecer una dirección MAC estática que incluya el prefijo de OUI de VMware si cumple el siguiente formato:

```
00:50:56:XX:YY:ZZ
```

Donde *XX* es un valor hexadecimal válido entre 00 y 3F, e *YY* y *ZZ* son valores hexadecimales válidos entre 00 y FF. Para evitar los conflictos con las direcciones MAC generadas por vCenter Server o asignadas a los adaptadores VMkernel para el tráfico de infraestructura, el valor de *XX* no puede ser mayor que 3F.

El valor máximo de una dirección MAC generada manualmente es el siguiente:

```
00:50:56:3F:FF:FF
```

Para evitar conflictos entre las direcciones MAC generadas y las asignadas manualmente, seleccione un valor exclusivo para *XX*:*YY*:*ZZ* entre las direcciones no modificables.

Asignar una dirección MAC estática mediante vSphere Web Client

Puede asignar direcciones MAC estáticas a la NIC virtual de una máquina virtual apagada desde vSphere Web Client.

Procedimiento

1 Ubique la máquina virtual en vSphere Web Client.

   a Seleccione un centro de datos, una carpeta, un clúster, un grupo de recursos o un host y haga clic en la pestaña **Máquinas virtuales**.

   b Haga clic en **Máquinas virtuales** y haga doble clic en la máquina virtual en la lista.

2 Apague la máquina virtual.

3 En la pestaña **Configurar** de la máquina virtual, expanda **Configuración** y seleccione **Hardware de máquina virtual**.

4 Haga clic en **Editar** y seleccione la pestaña **Hardware virtual** en el cuadro de diálogo que se muestra en la configuración.

5 En la pestaña **Hardware virtual**, expanda la sección del adaptador de red.

6 En Dirección MAC, seleccione **Manual** en el menú desplegable.

7 Escriba la dirección MAC estática y haga clic en **Aceptar**.

8 Encienda la máquina virtual.

Asignar una dirección MAC estática en el archivo de configuración de máquina virtual

Para establecer una dirección MAC estática para una máquina virtual, puede modificar el archivo de configuración de la máquina virtual a través de vSphere Web Client.

Procedimiento

1 Ubique la máquina virtual en vSphere Web Client.

   a Seleccione un centro de datos, una carpeta, un clúster, un grupo de recursos o un host y haga clic en la pestaña **Máquinas virtuales**.

   b Haga clic en **Máquinas virtuales** y haga doble clic en la máquina virtual en la lista.

2 Apague la máquina virtual.

3 En la pestaña **Configurar** de la máquina virtual, expanda **Configuración** y seleccione **Opciones de máquina virtual**.

4 Haga clic en **Editar** y expanda **Opciones avanzadas** de la pestaña **Opciones de máquina virtual** en el cuadro de diálogo que se muestra en la configuración.

5 Haga clic en **Editar configuración**.

6 Para asignar una dirección MAC estática, agregue o modifique los parámetros que corresponda.

Parámetro	Valor
`ethernet` *X* `.addressType`	**`estático`**
`ethernet` *X* `.address`	*MAC_address_of_the_virtual_NIC*

X junto a `ethernet` representa el número de secuencia de la NIC virtual en la máquina virtual.

Por ejemplo, el valor `0` en `ethernet0` representa la configuración del primer dispositivo de NIC virtual que se agregó a la máquina virtual.

7 Haga clic en **Aceptar**.

8 Encienda la máquina virtual.

Configurar vSphere para IPv6

13

Configure los hosts ESXi y vCenter Server para utilizarlos en un entorno IPv6 puro si desea obtener más espacio de direcciones y mejorar la asignación de direcciones.

IPv6 ha sido reconocido por el Grupo de trabajo de ingeniería de Internet (IETF) como el sucesor de IPv4 y ofrece los siguientes beneficios:

- Mayor longitud de direcciones. Al haber más espacio de direcciones, se soluciona el problema de agotamiento de las direcciones y se elimina la necesidad de traducción de direcciones de red. IPv6 utiliza direcciones de 128 bits, a diferencia de IPv4, que utiliza direcciones de 32 bits.
- Capacidad mejorada de configuración automática de direcciones en nodos.

Este capítulo incluye los siguientes temas:

Conectividad de vSphere IPv6

En un entorno basado en vSphere 6.0 y versiones posteriores, los nodos y las características se comunican de forma transparente a través de IPv6, tanto con una configuración de direcciones estática como automática.

IPv6 en la comunicación entre nodos de vSphere

Los nodos de una implementación de vSphere se comunican a través de IPv6 y aceptan direcciones asignadas según la configuración de red.

Tabla 13-1. Compatibilidad con IPv6 de los nodos en un entorno de vSphere

Tipo de conexión	Compatibilidad con IPv6	Configuración de direcciones de los nodos de vSphere
ESXi a ESXi	Sí	■ Estático ■ Automático: AUTOCONF/DHCPv6
Máquina vCenter Server a ESXi	Sí	■ Estático ■ Automático: AUTOCONF/DHCPv6
Máquina vCenter Server a máquina vSphere Web Client	Sí	■ Estático ■ Automático: AUTOCONF/DHCPv6
ESXi a máquina vSphere Client	Sí	■ Estático ■ Automático: AUTOCONF/DHCPv6
Máquina virtual a máquina virtual	Sí	■ Estático ■ Automático: AUTOCONF/DHCPv6
ESXi a almacenamiento iSCSI	Sí	■ Estático ■ Automático: AUTOCONF/DHCPv6
ESXi a almacenamiento NFS	Sí	■ Estático ■ Automático: AUTOCONF/DHCPv6
ESXi a Active Directory	No Use LDAP a través de vCenter Server para conectar ESXi a la base de datos de Active Directory	-
vCenter Server Appliance a Active Directory	No Use LDAP para conectar vCenter Server Appliance a la base de datos de Active Directory	-

Conectividad IPv6 de las características de vSphere

Ciertas características de vSphere no admiten IPv6:

- vSphere DPM a través de Intelligent Platform Management Interface (IPMI) y Hewlett-Packard Integrated Lights-Out (iLO). vSphere 6.5 solo admite Wake-On-LAN (WOL) para quitar un host del modo de espera.
- vSAN
- Authentication Proxy
- Utilice NFS 4.1 con AUTH_SYS.
- vSphere Management Assistant y vSphere Command-Line Interface con conexión a Active Directory.

  Use LDAP para conectar vSphere Management Assistant o vSphere Command-Line Interface a la base de datos de Active Directory.

Conectividad de IPv6 de las máquinas virtuales

Las máquinas virtuales pueden intercambiar datos de red a través de IPv6. vSphere admite la asignación estática y automática de direcciones IPv6 para máquinas virtuales.

También es posible configurar una o varias direcciones IPv6 al personalizar el sistema operativo invitado de una máquina virtual.

FQDN y direcciones IPv6

En vSphere, se deben usar los nombres de dominio completo (FQDN) asignados a las direcciones IPv6 del servidor DNS. Puede usar las direcciones IPv6 si tienen un FQDN válido en el servidor DNS para hacer búsquedas inversas.

Para implementar vCenter Server en un entorno IPv6 puro, se usan exclusivamente los FQDN.

Implementar vSphere en IPv6

Ejecute vSphere en un entorno de IPv6 puro para utilizar un espacio de direcciones extendido y la asignación de direcciones flexible.

Si planifica implementar hosts de vCenter Server y ESXi en una red IPv6, debe ejecutar pasos adicionales.

- Habilitar IPv6 en una instalación de vSphere

  Si tiene una implementación en entorno virgen de vSphere 6.5 en una red IPv6, configure IPv6 en los nodos de implementación y conéctelos para configurar ESXi y vCenter Server en una conexión de administración de IPv6 pura.

- Habilitar IPv6 en un entorno de vSphere actualizado

  En una implementación IPv4 de vSphere 6.5 que consta de una versión instalada o actualizada de vCenter Server y una versión actualizada de ESXi, configure ESXi y vCenter Server en una conexión de administración de IPv6 habilitando IPv6 en los nodos implementados y reconectándolos.

Habilitar IPv6 en una instalación de vSphere

Si tiene una implementación en entorno virgen de vSphere 6.5 en una red IPv6, configure IPv6 en los nodos de implementación y conéctelos para configurar ESXi y vCenter Server en una conexión de administración de IPv6 pura.

Requisitos previos

- Compruebe que las direcciones IPv6 para vCenter Server, los hosts ESXi y una base de datos externa, si se utiliza, estén asignados a nombres de dominio completo (FQDN) en el servidor DNS.
- Compruebe que la infraestructura de la red ofrezca conectividad IPv6 para los hosts ESXi, vCenter Server y la base de datos externa, si se utiliza.

- Compruebe que tenga instalada la versión 6.5 de vCenter Server con FQDN asignado a una dirección IPv6. Consulte la documentación de *Instalar y configurar vCenter Server*.
- Compruebe que los hosts tengan ESXi 6.5 instalado. Consulte la documentación de *Instalar y configurar vCenter Server*.

Procedimiento

1 En la interfaz del usuario de consola directa (DCUI), configure cada host ESXi como nodo IPv6 puro.

   a En la DCUI, presione F2 e inicie sesión en el host.

   b En el menú **Configurar red de administración**, seleccione **Configuración de IPv6** y presione Entrar.

   c Asigne una dirección IPv6 al host.

Opción de asignación de direcciones	Descripción
Asignación automática de direcciones con DHCPv6	1 Seleccione la opción **Usar configuración dinámica de direcciones y redes IPv6** y, a continuación, seleccione **Usar DHCPv6**. 2 Presione Entrar para guardar los cambios.
Asignación de direcciones estática	1 Seleccione la opción **Establecer configuración estática de direcciones y de redes IPv6** e introduzca la dirección IPv6 del host y de la puerta de enlace predeterminada. 2 Presione Entrar para guardar los cambios.

   d En el menú **Configurar red de administración**, seleccione **Configuración de IPv4** y presione Entrar.

   e Seleccione **Deshabilitar configuración IPv4 de la red de administración** y presione Entrar.

2 En vSphere Web Client, agregue los hosts al inventario.

Habilitar IPv6 en un entorno de vSphere actualizado

En una implementación IPv4 de vSphere 6.5 que consta de una versión instalada o actualizada de vCenter Server y una versión actualizada de ESXi, configure ESXi y vCenter Server en una conexión de administración de IPv6 habilitando IPv6 en los nodos implementados y reconectándolos.

Requisitos previos

- Compruebe que la infraestructura de la red ofrezca conectividad IPv6 para los hosts ESXi, vCenter Server y la base de datos externa, si se utiliza.
- Compruebe que las direcciones IPv6 para vCenter Server, los hosts ESXi y una base de datos externa, si se utiliza, estén asignados a nombres de dominio completo (FQDN) en el servidor DNS.

- Compruebe que la versión 6.x de vCenter Server esté instalada o actualizada. Consulte los documentos *Instalar y configurar vCenter Server* y *Actualizar vSphere*.
- Compruebe que todos los hosts ESXi se hayan actualizado a la versión 6.x. Consulte la documentación de *Actualizar vSphere*.

Procedimiento

1 En vSphere Web Client, desconecte los hosts de vCenter Server.

2 Configure cada host ESXi como un nodo IPv6 puro.

a Abra una conexión SSH e inicie sesión en el host ESXi.

b Ejecute el siguiente comando:

```
esxcli network ip interface ipv6 set -i vmk0 -e true
```

c Asigne una dirección IPv6 a la red de administración.

Opción de asignación de direcciones	Descripción

Asignación de direcciones estática	1 Abra una conexión SSH e inicie sesión en el host ESXi.
	2 Establezca una dirección IPv6 estática para la red de administración vmk0 ejecutando el siguiente comando:
	`esxcli network ip interface ipv6 address add -I IPv6_address -i vmk0`
	3 Establezca la puerta de enlace predeterminada para la red de administración vmk0 ejecutando el siguiente comando:
	`esxcli network ip interface ipv6 set -i vmk0 -g default_gateway_IPv6_address`
	4 Agregue un servidor DNS ejecutando el siguiente comando:
	`esxcli network ip dns server add -s DNS_server_IPv6_address`

Asignación automática de direcciones con DHCPv6	1 Abra una conexión SSH e inicie sesión en el host ESXi.
	2 Habilite DHCPv6 para la red de administración vmk0 ejecutando el siguiente comando:
	`esxcli network ip interface ipv6 -i vmk0 -enable-dhcpv6 = true`
	3 Habilite el enrutador IPv6 anunciado para la red de administración vmk0 ejecutando el siguiente comando:
	`esxcli network ip interface ipv6 set -i vmk0 -enable-router-adv =true`
	4 Agregue un servidor DNS o utilice la configuración de DNS publicada por DHCPv6 ejecutando uno de los siguientes comandos:
	`esxcli network ip dns server add -s DNS_server_IPv6_address`
	`esxcli network ip interface ipv6 set -i vmk0 --peer-dns=true`

3 Deshabilite la configuración de IPv4 para la red de administración.

   a Abra una conexión SSH e inicie sesión en el host ESXi.

   b Ejecute el siguiente comando:

   ```
   esxcli network ip interface ipv4 set -i vmk0 --type=none
   ```

4 Si vCenter Server utiliza una base de datos externa, configúrela como un nodo IPv6.

5 Configure vCenter Server como un nodo IPv6 puro y reinícielo.

6 Deshabilite IPv4 en el servidor de base de datos.

7 En vSphere Web Client, agregue los hosts al inventario.

8 Deshabilite IPv4 en la infraestructura de red.

Habilitar o deshabilitar la compatibilidad con IPv6 en un host

La compatibilidad con IPv6 en vSphere permite que los hosts funcionen en una red IPv6 con un espacio de direcciones amplio, multidifusión avanzada y enrutamiento simplificado, entre otras características.

En ESXi 5.1 y versiones posteriores, IPv6 está habilitado de forma predeterminada.

Procedimiento

1 En vSphere Web Client, desplácese hasta el host.

2 En la pestaña **Configurar**, expanda **Redes** y seleccione **Opciones avanzadas**.

3 Haga clic en **Editar**.

4 En el menú desplegable **Compatibilidad con IPv6**, habilite o deshabilite la compatibilidad con IPv6.

5 Haga clic en **Aceptar**.

6 Reinicie el host para aplicar los cambios en la compatibilidad con IPv6.

Pasos siguientes

Configure las opciones de IPv6 de los adaptadores VMkernel en el host, por ejemplo, de la red de administración. Consulte Configurar IPv6 en un host ESXi.

Configurar IPv6 en un host ESXi

Para conectar un host ESXi a través de IPv6 a redes de administración, vSphere vMotion, almacenamiento compartido, vSphere Fault Tolerance y otras funciones, edite la configuración de IPv6 de los adaptadores VMkernel en el host.

Requisitos previos

Compruebe que IPv6 esté habilitado en el host ESXi. Consulte Habilitar o deshabilitar la compatibilidad con IPv6 en un host .

Procedimiento

1 En vSphere Web Client, desplácese hasta el host.

2 En la pestaña**Configurar**, expanda **Redes** y seleccione **Adaptadores de VMKernel**.

3 Seleccione el adaptador VMkernel en el conmutador distribuido o estándar de destino y, a continuación, haga clic en **Editar**.

4 En el cuadro de diálogo Editar configuración, haga clic en **Configuración de IPv6**.

5 Configure la asignación de direcciones del adaptador VMkernel.

Opción de dirección IPv6	Descripción
Obtener la dirección IPv6 automáticamente por medio de DHCP	Se recibe una dirección IPv6 para el adaptador VMkernel desde un servidor DHCPv6.
Obtener la dirección IPv6 automáticamente por medio del anuncio de enrutador	Se recibe una dirección IPv6 para el adaptador VMkernel desde un enrutador por medio del anuncio.
Direcciones IPv6 estáticas	Establezca una o más direcciones. Para cada entrada de dirección, introduzca la dirección IPv6 del adaptador, la longitud del prefijo de subred y la dirección IPv6 de la puerta de enlace predeterminada.

Puede seleccionar varias opciones de asignación según la configuración de la red.

6 (opcional) En la sección Configuración avanzada de la página de configuración de IPv6, quite ciertas direcciones IPv6 asignadas por medio del anuncio de enrutador.

Puede eliminar ciertas direcciones IPv6 que el host obtuvo por medio del anuncio de enrutador para detener la comunicación con estas direcciones. También puede eliminar todas las direcciones asignadas automáticamente para aplicar las direcciones estáticas configuradas en el VMkernel.

7 Haga clic en **Aceptar** para aplicar los cambios en el adaptador VMkernel.

Configurar IPv6 en vCenter Server

Configure vCenter Server para la comunicación con los hosts ESXi y con vSphere Web Client en una red IPv6.

Configurar IPv6 en vCenter Server Appliance

Use vSphere Web Client para configurar vCenter Server Appliance para la comunicación con los hosts ESXi en una red IPv6.

Procedimiento

1 En la página principal de vSphere Web Client, pase el cursor sobre el icono **Inicio**, haga clic en **Inicio** y seleccione **Configuración del sistema**.

2 En Configuración del sistema, haga clic en **Nodos**.

3 En Nodos, seleccione un nodo y haga clic en la pestaña **Administrar**.

4 En Común, seleccione **Redes** y haga clic en **Editar**.

5 Expanda el nombre de la interfaz de red para editar la configuración de la dirección IP.

6 Edite la configuración de IPv6.

Opción	Descripción
Obtener la configuración de IPv6 automáticamente a través de DHCP	Asigna automáticamente direcciones IPv6 al dispositivo desde la red mediante DHCP.
Obtener la configuración de IPv6 automáticamente por medio del anuncio de enrutador	Asigna automáticamente direcciones IPv6 al dispositivo desde la red mediante un anuncio de enrutador.
Direcciones IPv6 estáticas	Usa direcciones IPv6 estáticas que se configuran manualmente. 1 Haga clic en el icono **Agregar**. 2 Ingrese la dirección IPv6 y la longitud del prefijo de subred. 3 Haga clic en **Aceptar**. 4 (Opcional) Edite la puerta de enlace predeterminada.

Puede configurar el dispositivo para obtener automáticamente la configuración de IPv6 por medio de DHCP y del anuncio de enrutador. Puede asignar una dirección IPv6 estática al mismo tiempo.

7 (opcional) Para quitar direcciones IPv6 que estén asignadas automáticamente a través del anuncio del enrutador, haga clic en **Quitar direcciones** y elimine las direcciones.

En algunos casos, es necesario eliminar ciertas direcciones IPv6 que vCenter Server Appliance obtuvo a través del anuncio del enrutador a fin de detener la comunicación con estas direcciones y aplicar las direcciones estáticas configuradas.

Pasos siguientes

Conecte los hosts ESXi para vCenter Server en IPv6 según sus FQDN.

Configurar vCenter Server en Windows con IPv6

Para conectar hosts ESXi o vSphere Web Client por IPv6 a una instancia de vCenter Server que se ejecuta en un equipo host de Windows, configure las opciones de la dirección IPv6 en Windows.

Procedimiento

◆ En la carpeta Centro de redes y recursos compartidos del panel de control de Windows, configure las opciones de la dirección IPv6 del host para la conexión de área local.

Pasos siguientes

Conecte los hosts ESXi para vCenter Server en IPv6 según sus FQDN.

Supervisar conexión y tráfico de la red

14

Puede supervisar la conexión de red y los paquetes que se transmiten por los puertos de vSphere Standard Switch o vSphere Distributed Switch a fin de analizar el tráfico entre las máquinas virtuales y los hosts.

Este capítulo incluye los siguientes temas:

Capturar paquetes de red mediante la utilidad PacketCapture

Use la utilidad PacketCapture para diagnosticar problemas de redes, como conexión lenta, pérdida de paquetes y problemas de conectividad.

PacketCapture es una utilidad ligera tcpdump que captura y almacena solo la cantidad mínima de datos necesaria para diagnosticar el problema de red. PacketCapture está integrado en el servicio rhttpproxy de ESXi y vCenter Server Appliance. Para iniciar y detener PacketCapture, se debe editar el archivo de configuración XML del servicio rhttpproxy.

Procedimiento

1 Inicie la captura de paquetes.

   a Abra una conexión SSH e inicie sesión en el host ESXi o en vCenter Server Appliance.

   b Abra el archivo `config.xml` para editarlo.

Componente de vSphere	Ubicación del archivo
ESXi	`/etc/vmware/rhttpproxy/config.xml`
vCenter Server Appliance	`/etc/vmware-rhttpproxy/config.xml`

c Realice los siguientes cambios.

```
<config>
  <packetCapture>
    <enabled>true</enabled>
```

d (opcional) Configure las opciones de PacketCapture.

Opción y valor predeterminado	Descripción
<validity>72</validity>	En el inicio, elimine todos los archivos `pcap` y `pcap.gz` que se modificaron por última vez antes del periodo de horas especificado y que no forman parte del proceso actual.
<directory>/directory_path</directory>	El directorio en el que se almacenan los archivos `pcap` y `pcap.gz`. El directorio debe existir y debe ser posible acceder a él.
<maxDataInPcapFile>52428800</maxDataInPcapFile>	La cantidad de datos capturados en bytes que puede almacenar cada archivo `pcap` y `pcap.gz` antes de pasar al siguiente archivo. El tamaño mínimo es de 5 MB en vCenter Server Appliance y de 2,5 MB en ESXi. **Nota** El almacenamiento de 50 MB de datos capturados en un archivo `pcap` requiere un archivo `pcap` de aproximadamente 67,5 MB.
<maxPcapFilesCount>5</maxPcapFilesCount>	El número de archivos `pcap` o `pcap.gz` que desea rotar. La cantidad mínima es de 2.

e Guarde y cierre el archivo `config.xml`.

f Vuelva a cargar el archivo `config.xml` ejecutando el siguiente comando.

```
kill -SIGHUP `pidof rhttpproxy`
```

2 Detenga la captura de paquetes.

a Abra una conexión SSH e inicie sesión en el host ESXi o en vCenter Server Appliance.

b Abra el archivo `config.xml` para editarlo.

c Realice los siguientes cambios.

```
<config>
  <packetCapture>
    <enabled>false</enabled>
```

d Guarde y cierre el archivo `config.xml`.

e Vuelva a cargar el archivo `config.xml` ejecutando el siguiente comando.

```
kill -SIGHUP `pidof rhttpproxy`
```

3 Recopile los datos capturados.

Los archivos `pcap` o `pcap.gz` se almacenan en los siguientes directorios predeterminados.

Componente de vSphere	Ubicación del archivo
ESXi	`/var/run/log`
vCenter Server Appliance	`/var/log/vmware/rhttpproxy`

Pasos siguientes

Copie los archivos `pcap` y `pcap.gz` en un sistema que ejecute una herramienta de análisis de red (p. ej., Wireshark) y examine los detalles del paquete.

Antes de analizar los archivos `pcap` y `pcap.gz` capturados de un host ESXi, use la utilidad de TraceWrangler para corregir los metadatos de tamaño de trama. Para obtener más información, consulte https://kb.vmware.com/kb/52843.

Capturar y rastrear paquetes de red mediante la utilidad pktcap-uw

Puede supervisar el tráfico que pasa por los adaptadores de red físicos, los adaptadores VMkernel y los adaptadores de máquinas virtuales y analizar información sobre los paquetes desde la interfaz de usuario gráfica de las herramientas de análisis de red como Wireshark.

En vSphere 5.5 o versiones posteriores, puede supervisar los paquetes de un host a través de la utilidad de consola `pktcap-uw`. Puede utilizar la utilidad sin instalación adicional en un host ESXi. `pktcap-uw` permite supervisar el tráfico en varios puntos de la pila de red del host.

Para hacer un análisis detallado de los paquetes capturados, puede guardar el contenido de los paquetes desde la utilidad `pktcap-uw` en archivos con formato PCAP o PCAPNG y abrirlos en Wireshark. También puede solucionar problemas de paquetes descartados y rastrear la ruta de un paquete dentro de la pila de red.

Nota La utilidad `pktcap-uw` no tiene compatibilidad total con las versiones anteriores de vSphere. Las opciones de la utilidad están sujetas a cambios.

Sintaxis del comando pktcap-uw para capturar paquetes

Use la utilidad `pktcap-uw` para inspeccionar el contenido de los paquetes mientras atraviesan la pila de red en un host ESXi.

Sintaxis pktcap-uw para capturar paquetes

El comando `pktcap-uw` tiene la siguiente sintaxis para capturar paquetes en un determinado lugar en la pila de red:

```
pktcap-uw
```

```
        switch_port_arguments
        capture_point_options
        filter_options
        output_control_options
```

Nota Ciertas opciones de la utilidad `pktcap-uw` están diseñadas solo para uso interno de VMware y se deben usar solo bajo la supervisión del soporte técnico de VMware. Esas opciones no se describen en la guía *Redes de vSphere*.

Tabla 14-1. Argumentos pktcap-uw para capturar paquetes

Grupo de argumento	Argumento	Descripción
switch_port_arguments	`--uplink vmnicX`	Capturan paquetes que están relacionados con un adaptador físico. Se pueden combinar las opciones `--uplink` y `--capture` para supervisar los paquetes en una determinada ubicación en la ruta de acceso entre el adaptador físico y el conmutador virtual. Consulte Capturar paquetes que llegan a un adaptador físico.
	`--vmk vmkX`	Capturan paquetes que están relacionados con un adaptador VMkernel. Se pueden combinar las opciones `vmk` y `--capture` para supervisar los paquetes en una determinada ubicación en la ruta de acceso entre el adaptador VMkernel y el conmutador virtual. Consulte Capturar paquetes para un adaptador VMkernel.

Tabla 14-1. Argumentos pktcap-uw para capturar paquetes (continuación)

Grupo de argumento	Argumento	Descripción
	`--switchport {`*`vmxnet3_port_ID`*` | `*`vmkernel_adapter_port_ID`*`}`	Capturan paquetes que están relacionados con un adaptador de máquina virtual VMXNET3 o con un adaptador VMkernel que está conectado al puerto de un conmutador virtual determinado. Puede ver el identificador del puerto en el panel de red de la utilidad `esxtop`. Se pueden combinar las opciones `switchport` y `capture` para supervisar los paquetes en una determinada ubicación en la ruta de acceso entre el adaptador VMXNET3 o el adaptador VMkernel y el conmutador virtual. Consulte Capturar paquetes para un adaptador de máquina virtual VMXNET3.
	`--lifID `*`lif_ID`*	Capturan paquetes que están relacionados con la interfaz lógica de un enrutador distribuido. Consulte la documentación de *VMware NSX*.
capture_point_options	`--capture `*`capture_point`*	Capturan paquetes en una ubicación determinada de la pila de red. Por ejemplo, es posible supervisar los paquetes justo después de que llegan desde un adaptador físico.
	`--dir {0|1}`	Capturan paquetes de acuerdo con la dirección del flujo con respecto al conmutador virtual. 0 representa el tráfico de entrada y 1 el tráfico saliente. De forma predeterminada, la utilidad `pktcap-uw` captura el tráfico de ingreso. Utilice la opción `--dir` junto con la opción `--uplink`, `--vmk`, o bien `--switchport`.

Tabla 14-1. Argumentos pktcap-uw para capturar paquetes (continuación)

Grupo de argumento	Argumento	Descripción
	`--stage {0|1}`	Capturan el paquete más cerca de su origen o de su destino. Utilice esta opción para examinar cómo un paquete cambia mientras atraviesa los puntos en la pila. 0 representa el tráfico más cerca del origen y 1 el tráfico más cerca del destino. Utilice la opción `--stage` junto con la opción `--uplink`, `--vmk`, `--switchport`, o bien `--dvfilter`.
	`--dvfilter` *filter_name* `--capture PreDVFilter|PostDVFilter`	Capturan paquetes antes o después de que los intercepte vSphere Network Appliance (DVFilter). Consulte Capturar paquetes en el nivel DVFilter.
	`-A	--availpoints`	Vea todos los puntos de captura que admite la utilidad `pktcap-uw`.
	Para obtener más información sobre los puntos de captura de la utilidad `pktcap-uw`, consulte Puntos de captura de la utilidad pktcap-uw.	
filter_options	Filtran paquetes capturados de acuerdo con la dirección de origen o destino, identificador de VLAN, identificador de VXLAN, protocolo de Capa 3 y puerto TCP. Consulte Opciones de pktcap-uw para el filtrado de paquetes.	
output_control_options	Guardan el contenido de un paquete en un archivo, capturan solamente una cantidad de paquetes y capturan una cantidad de bytes en el comienzo de los paquetes y así sucesivamente. Consulte Opciones de pktcap-uw para control de salida.	

Las barras verticales (|) representan valores alternativos, y las llaves ({}) utilizadas en combinación con barras verticales especifican una lista de opciones correspondientes a un argumento o a una opción.

Sintaxis del comando pktcap-uw para el rastreo de paquetes

La utilidad `pktcap-uw` permite ver la ruta de acceso de un paquete en la pila de red de un host ESXi para realizar un análisis de latencia.

Sintaxis de pktcap-uw para el rastreo de paquetes

El comando de la utilidad `pktcap-uw` tiene la siguiente sintaxis si el objetivo es rastrear paquetes en la pila de red:

```
pktcap-uw --trace filter_optionsoutput_control_options
```

Opciones de la utilidad pktcap-uw para el rastreo de paquetes

La utilidad `pktcap-uw` ofrece las siguientes opciones si el objetivo es rastrear paquetes:

Tabla 14-2. Opciones de pktcap-uw para el rastreo de paquetes

Argumento	Descripción
filter_options	Se filtran los paquetes rastreados según la dirección de origen o de destino, el identificador de VLAN, el identificador de VXLAN, el protocolo de Capa 3 y el puerto TCP. Consulte Opciones de pktcap-uw para el filtrado de paquetes.
output_control_options	Se guarda el contenido de un paquete en un archivo y se rastrea una cantidad limitada de paquetes. Consulte Opciones de pktcap-uw para control de salida.

Opciones de pktcap-uw para control de salida

Utilice las opciones de control de salida de la utilidad `pktcap-uw` para guardar el contenido del paquete en un archivo, capturar una cierta cantidad de bytes de cada paquete y limitar la cantidad de paquetes capturados.

Opciones de pktcap-uw para control de salida

Las opciones de la utilidad `pktcap-uw` para el control de salida son válidas cuando se capturan y rastrean paquetes. Para obtener información sobre la sintaxis de comandos de la utilidad `pktcap-uw`, consulte Sintaxis del comando pktcap-uw para capturar paquetes y Sintaxis del comando pktcap-uw para el rastreo de paquetes.

Tabla 14-3. Opciones de control de salida compatibles con la utilidad pktcap-uw

Opción	Descripción
`{-o	--outfile}` *`pcap_file`*	Guarde los paquetes capturados o rastreados en un archivo con formato de captura de paquetes (PCAP). Utilice esta opción para examinar los paquetes en una herramienta de análisis visual, como Wireshark.
`-P` | `--ng`	Guarde el contenido del paquete en un archivo con formato PCAPNG. Utilice esta opción junto con `-o` o `--outfile`.
`--console`	Imprima los detalles y el contenido del paquete en la salida de la consola. De forma predeterminada, la utilidad `pktcap-uw` muestra la información del paquete en la salida de la consola.
`{-c	--count}` *`number_of_packets`*	Capture los primeros paquetes *number_of_packets*.

Tabla 14-3. Opciones de control de salida compatibles con la utilidad pktcap-uw (continuación)

Opción	Descripción
`{-s | --snaplen} snapshot_length`	Capture solamente los primeros bytes de *snapshot_length* de cada paquete. Si el tráfico del host es intenso, utilice esta opción para reducir la carga en la CPU y el almacenamiento. Para limitar el tamaño del contenido capturado, establezca un valor mayor que 24. Para capturar el paquete completo, establezca la opción en 0.
`-h`	Vea información de ayuda sobre la utilidad `pktcap-uw`.

Las barras verticales (|) representan valores alternativos, y las llaves ({}) utilizadas en combinación con barras verticales especifican una lista de opciones correspondientes a un argumento o a una opción.

Opciones de pktcap-uw para el filtrado de paquetes

Se puede limitar el rango de paquetes que se supervisan mediante la utilidad `pktcap-uw` a fin de aplicar opciones de filtrado para direcciones de origen y destino, VLAN, VXLAN y el protocolo de siguiente nivel que consume la carga útil del paquete.

Opciones de filtros

Las opciones de filtros para `pktcap-uw` son válidas cuando se capturan y se rastrean paquetes. Para obtener información sobre la sintaxis de comandos de la utilidad `pktcap-uw`, consulte Sintaxis del comando pktcap-uw para capturar paquetes y Sintaxis del comando pktcap-uw para el rastreo de paquetes.

Tabla 14-4. Opciones de filtros de la utilidad pktcap-uw

Opción	Descripción
`--srcmac mac_address`	Capture o rastree paquetes que tengan una dirección MAC de origen específica. Separe los octetos con dos puntos (:).
`--dstmac mac_address`	Capture o rastree paquetes que tengan una dirección MAC de destino específica. Separe los octetos con dos puntos (:).
`--mac mac_address`	Capture o rastree paquetes que tengan una dirección MAC de origen o de destino específica. Separe los octetos con dos puntos (:).

Tabla 14-4. Opciones de filtros de la utilidad pktcap-uw (continuación)

Opción	Descripción
`--ethtype 0x`*`EtherType`*	Capture o rastree paquetes en la Capa 2 de acuerdo con el protocolo de siguiente nivel que consume la carga útil del paquete. *EtherType* corresponde al campo EtherType en tramas Ethernet. Representa el tipo de protocolo de siguiente nivel que consume la carga útil de la trama. Por ejemplo, para supervisar el tráfico del protocolo Link Layer Discovery Protocol (LLDP), escriba **`--ethtype 0x88CC`**.
`--vlan` *`VLAN_ID`*	Capture o rastree paquetes que pertenecen a una VLAN.
`--srcip` *`IP_addess|IP_address/subnet_range`*	Capture o rastree paquetes que tengan una subred o una dirección IPv4 de origen específicas.
`--dstip` *`IP_addess|IP_address/subnet_range`*	Capture o rastree paquetes que tengan una subred o una dirección IPv4 de destino específicas.
`--ip` *`IP_addess`*	Capture o rastree paquetes que tengan una subred o una dirección IPv4 de origen o de destino específicas.
`--proto 0x`*`IP_protocol_number`*	Capture o rastree paquetes en la Capa 3 de acuerdo con el protocolo de siguiente nivel que consume la carga útil. Por ejemplo, para supervisar el tráfico del protocolo UDP, escriba **`--proto 0x11`**.
`--srcport` *`source_port`*	Capture o rastree paquetes de acuerdo con el puerto TCP de origen.
`--dstport` *`destination_port`*	Capture o rastree paquetes de acuerdo con el puerto TCP de destino.
`--tcpport` *`TCP_port`*	Capture o rastree paquetes de acuerdo con el puerto TCP de origen o de destino.
`--vxlan` *`VXLAN_ID`*	Capture o rastree paquetes que pertenecen a una VXLAN.

Las barras verticales | representan valores alternativos.

Captura de paquetes mediante la utilidad pktcap-uw

Capture paquetes a través de la utilidad `pktcap-uw` en la ruta entre un conmutador virtual y los adaptadores físicos, los adaptadores VMkernel y los adaptadores de máquina virtual para solucionar problemas de transferencia de datos en la pila de red de un host ESXi.

Capturar paquetes que llegan a un adaptador físico

Supervise el tráfico de host relacionado con la red externa mediante la captura de paquetes en ciertos puntos de la ruta de acceso entre vSphere Standard Switch o vSphere Distributed Switch y un adaptador físico.

Puede especificar un determinado punto de captura en la ruta de acceso de datos entre un conmutador virtual y un adaptador físico, o determinar un punto de captura por la dirección del tráfico en relación con el conmutador y la proximidad al origen o al destino de los paquetes. Para obtener información sobre los puntos de captura compatibles, consulte Puntos de captura de la utilidad pktcap-uw.

Procedimiento

1 (opcional) Busque el nombre del adaptador físico que desea supervisar en la lista de adaptadores de host.

   - En vSphere Web Client, en la pestaña **Configurar** correspondiente al host, expanda **Redes** y seleccione **Adaptadores físicos**.
   - En ESXi Shell del host, ejecute el siguiente comando ESXCLI para ver una lista de los adaptadores físicos y examinar su estado:

     ```
     esxcli network nic list
     ```

   Cada adaptador físico se representa como `vmnicX`. *X* es el número que ESXi le asigna al puerto del adaptador físico.

2 En ESXi Shell del host, ejecute el comando `pktcap-uw` con el argumento `--uplink vmnicX` y con opciones para supervisar los paquetes en un punto determinado, filtrar paquetes capturados y guardar el resultado en un archivo.

   ```
               pktcap-uw
               --uplink vmnicX [--capturecapture_point|--dir 0|1]  [filter_options]
   [--outfilepcap_file_path [--ng]] [--countnumber_of_packets]
   ```

   donde los corchetes ([]) encierran las opciones del comando `pktcap-uw--uplink vmnicX` y las barras verticales | representan valores alternativos.

Si ejecuta el comando `pktcap-uw--uplink vmnicX` sin opciones, obtendrá el contenido de los paquetes que entran al conmutador estándar o distribuido en la salida de la consola en el punto donde se conmutan.

a Utilice la opción `--capture` para revisar los paquetes en otro punto de captura, o la opción `--dir` para revisarlos en otra dirección del tráfico.

Comando opción pktcap-uw	Objetivo
--capture UplinkSnd	Supervisa los paquetes inmediatamente antes de que entren en el dispositivo de adaptador físico.
--capture UplinkRcv	Supervisa los paquetes inmediatamente después de que se reciban en la pila de red desde el adaptador físico.
--dir 1	Supervisa los paquetes que salen del conmutador virtual.
--dir 0	Supervisa los paquetes que entran en el conmutador virtual.

b Utilice *filter_options* para filtrar paquetes según la dirección de origen y destino, identificador de VLAN, identificador de VXLAN, protocolo de Capa 3 y puerto TCP.

Por ejemplo, para supervisar paquetes de un sistema de origen con la dirección IP 192.168.25.113, utilice la opción de filtro `--srcip 192.168.25.113`.

c Utilice las opciones para guardar el contenido de cada paquete o el contenido de una cantidad limitada de paquetes en un archivo `.pcap` o `.pcapng`.

- Para guardar paquetes en un archivo `.pcap`, utilice la opción `--outfile`.
- Para guardar los paquetes en un archivo `.pcapng`, utilice las opciones `--ng` y `--outfile`.

Puede abrir el archivo en una herramienta de análisis de red como Wireshark.

De forma predeterminada, la utilidad `pktcap-uw` guarda los archivos de paquete en la carpeta raíz del sistema de archivos de ESXi.

d Utilice la opción `--count` para supervisar solo una cantidad de paquetes.

3 Si no limitó la cantidad de paquetes con la opción `--count`, presione Ctrl+C para dejar de capturar o rastrear paquetes.

Ejemplo: Capturar paquetes que se reciben en vmnic0 desde una dirección IP 192.168.25.113

Para capturar los primeros 60 paquetes de un sistema de origen al que se asigna la dirección IP 192.168.25.113 en vmnic0, y guardarlos en un archivo llamado `vmnic0_rcv_srcip.pcap`, ejecute el siguiente comando `pktcap-uw`:

```
 pktcap-uw --uplink vmnic0 --capture UplinkRcv --srcip 192.168.25.113 --outfile
vmnic0_rcv_srcip.pcap --count 60
```

Pasos siguientes

Si el contenido del paquete se guarda en un archivo, copie el archivo del host ESXi al sistema que ejecuta una herramienta de análisis gráfico, como Wireshark, y ábralo en la herramienta para examinar los detalles del paquete.

Capturar paquetes para un adaptador de máquina virtual VMXNET3

Supervise el tráfico que circula entre un conmutador virtual y un adaptador de máquina virtual VMXNET3 mediante la utilidad `pktcap-uw`.

Se puede especificar un determinado punto de captura en la ruta de acceso de los datos entre un conmutador virtual y un adaptador de máquina virtual. También puede determinar un punto de captura por la dirección del tráfico en relación con el conmutador y con la proximidad al origen o destino de los paquetes. Para obtener información sobre los puntos de captura compatibles, consulte Puntos de captura de la utilidad pktcap-uw.

Requisitos previos

Compruebe que el adaptador de máquina virtual sea de tipo VMXNET3.

Procedimiento

1 Conozca el identificador de puerto del adaptador de la máquina virtual en el host mediante la utilidad `esxtop`.

   a En ESXi Shell del host, ejecute `esxtop` para iniciar la utilidad.

   b Para cambiar al panel de red de la utilidad, presione N.

   c En la columna Utilizado por, ubique el adaptador de la máquina virtual y escriba el valor Identificador de puerto correspondiente.

      El campo USED-BY contiene el nombre de la máquina virtual y el puerto al cual está conectado el adaptador de la máquina virtual.

   d Presione Q para salir de `esxtop`.

2 En ESXi Shell, ejecute `pktcap-uw --switchport` *`port_ID`*.

   port_ID es el identificador que muestra la utilidad `esxtop` respecto del adaptador de la máquina virtual en la columna PORT-ID.

3 En ESXi Shell, ejecute el comando `pktcap-uw` con el argumento `--switchport` *`port_ID`* y las opciones para supervisar paquetes en un punto determinado, filtrar paquetes capturados y guardar el resultado en un archivo.

```
pktcap-uw --switchport port_ID [--capture capture_point|--dir 0|1 --stage 0|1]
[filter_options] [--outfile pcap_file_path [--ng]] [--count number_of_packets]
```

   donde los corchetes ([]) encierran las opciones del comando `pktcap-uw --switchport` *`port_ID`* y las barras verticales | representan valores alternativos.

Si ejecuta el comando `pktcap-uw --switchport port_ID` sin opciones, obtiene el contenido de los paquetes que entran al conmutador estándar o distribuido en la salida de la consola en el punto donde se conmutan.

a Para comprobar los paquetes en otro punto de captura u otra dirección en la ruta de acceso entre el sistema operativo invitado y el conmutador virtual, utilice la opción `--capture` o combine los valores de las opciones `--dir` y `--stage`.

Opciones de comando pktcap-uw	Objetivo
--capture VnicTx	Supervise los paquetes cuando pasan de la máquina virtual al conmutador.
--capture VnicRx	Supervise los paquetes cuando llegan a la máquina virtual.
--dir 1 --stage 0	Supervisa los paquetes inmediatamente después de salir del conmutador virtual.
--dir 1	Supervise los paquetes inmediatamente antes de que entren en la máquina virtual.
--dir 0 --stage 1	Supervise los paquetes inmediatamente después de que entren en el conmutador virtual.

b Utilice *filter_options* para filtrar paquetes según la dirección de origen y destino, identificador de VLAN, identificador de VXLAN, protocolo de Capa 3 y puerto TCP.

Por ejemplo, para supervisar paquetes de un sistema de origen con la dirección IP 192.168.25.113, utilice la opción de filtro `--srcip 192.168.25.113`.

c Utilice las opciones para guardar el contenido de cada paquete o el contenido de una cantidad limitada de paquetes en un archivo `.pcap` o `.pcapng`.

- Para guardar paquetes en un archivo `.pcap`, utilice la opción `--outfile`.
- Para guardar los paquetes en un archivo `.pcapng`, utilice las opciones `--ng` y `--outfile`.

Puede abrir el archivo en una herramienta de análisis de red como Wireshark.

De forma predeterminada, la utilidad `pktcap-uw` guarda los archivos de paquete en la carpeta raíz del sistema de archivos de ESXi.

d Utilice la opción `--count` para supervisar solo una cantidad de paquetes.

4 Si no limitó la cantidad de paquetes con la opción `--count`, presione Ctrl+C para dejar de capturar o rastrear paquetes.

Ejemplo: Capturar paquetes que se reciben en una máquina virtual desde una dirección IP 192.168.25.113

Para capturar los primeros 60 paquetes de un origen al que se asigna la dirección IP 192.168.25.113 cuando llegan al adaptador de una máquina virtual con el identificador de puerto 33554481 y guardarlos en un archivo llamado `vmxnet3_rcv_srcip.pcap`, ejecute el siguiente comando `pktcap-uw`:

```
 pktcap-uw --switchport 33554481 --capture VnicRx --srcip 192.168.25.113 --outfile
vmxnet3_rcv_srcip.pcap --count 60
```

Pasos siguientes

Si el contenido del paquete se guarda en un archivo, copie el archivo del host ESXi al sistema que ejecuta una herramienta de análisis gráfico, como Wireshark, y ábralo en la herramienta para examinar los detalles del paquete.

Capturar paquetes para un adaptador VMkernel

Supervise los paquetes que se intercambian entre un adaptador VMkernel y un conmutador virtual mediante la utilidad `pktcap-uw`.

Es posible capturar paquetes en un determinado punto de captura en el flujo entre un conmutador virtual y un adaptador VMkernel. También puede determinar un punto de captura por la dirección del tráfico en relación con el conmutador y con la proximidad al origen o destino de los paquetes. Para obtener información sobre los puntos de captura compatibles, consulte Puntos de captura de la utilidad pktcap-uw.

Procedimiento

1 (opcional) Busque el nombre del adaptador VMkernel que desea supervisar en la lista de adaptadores VMkernel.

- En vSphere Web Client, expanda **Redes** en la pestaña **Configurar** para el host y seleccione **Adaptadores de VMkernel**.
- En ESXi Shell del host, ejecute el siguiente comando de consola para ver una lista de los adaptadores físicos:

```
esxcli network ip interface list
```

Cada adaptador VMkernel se representa como `vmkX`, donde *X* es el número de secuencia que ESXi asignó al adaptador.

2 En ESXi Shell del host, ejecute el comando `pktcap-uw` con el argumento `--vmk vmkX` y las opciones para supervisar paquetes en un punto determinado, filtrar paquetes capturados y guardar el resultado en un archivo.

```
            pktcap-uw
            --vmk vmkX [--capturecapture_point|--dir 0|1 --stage 0|1]  [filter_options]
[--outfilepcap_file_path [--ng]] [--countnumber_of_packets]
```

donde los corchetes ([]) encierran las opciones del comando `pktcap-uw--vmk vmkX` y las barras verticales | representan valores alternativos.

Puede reemplazar la opción `--vmk vmkX` con `--switchportvmkernel_adapter_port_ID`, donde *vmkernel_adapter_port_ID* es el valor PORT-ID que el panel de red de la utilidad `esxtop` muestra para el adaptador.

Si ejecuta el comando `pktcap-uw--vmk vmkX` sin opciones, obtendrá el contenido de los paquetes que están dejando el adaptador VMkernel.

a Para comprobar los paquetes transmitidos o recibidos en el lugar y la dirección específica, utilice la opción `--capture` o combine los valores de las opciones `--dir` y `--stage`.

Opciones de comando pktcap-uw	Objetivo
--dir 1 **--stage** 0	Supervisa los paquetes inmediatamente después de salir del conmutador virtual.
--dir 1	Supervisa los paquetes inmediatamente antes de que entren en el adaptador VMkernel.
--dir 0 **--stage** 1	Supervisa los paquetes inmediatamente antes de que entren en el conmutador virtual.

b Utilice *filter_options* para filtrar paquetes según la dirección de origen y destino, identificador de VLAN, identificador de VXLAN, protocolo de Capa 3 y puerto TCP.

Por ejemplo, para supervisar paquetes de un sistema de origen con la dirección IP 192.168.25.113, utilice la opción de filtro `--srcip 192.168.25.113`.

c Utilice las opciones para guardar el contenido de cada paquete o el contenido de una cantidad limitada de paquetes en un archivo `.pcap` o `.pcapng`.

- Para guardar paquetes en un archivo `.pcap`, utilice la opción `--outfile`.
- Para guardar los paquetes en un archivo `.pcapng`, utilice las opciones `--ng` y `--outfile`.

Puede abrir el archivo en una herramienta de análisis de red como Wireshark.

De forma predeterminada, la utilidad `pktcap-uw` guarda los archivos de paquete en la carpeta raíz del sistema de archivos de ESXi.

d Utilice la opción `--count` para supervisar solo una cantidad de paquetes.

3 Si no limitó la cantidad de paquetes con la opción `--count`, presione Ctrl+C para dejar de capturar o rastrear paquetes.

Pasos siguientes

Si el contenido del paquete se guarda en un archivo, copie el archivo del host ESXi al sistema que ejecuta una herramienta de análisis gráfico, como Wireshark, y ábralo en la herramienta para examinar los detalles del paquete.

Capturar paquetes descartados

La utilidad `pktcap-uw` permite solucionar problemas de pérdida de conectividad mediante la captura de paquetes descartados.

A veces se descartan paquetes en un punto de la transmisión de red por diferentes motivos, por ejemplo, debido a una regla de firewall, al filtrado de IOChain y DVfilter, a la falta de coincidencia de VLAN, a un problema de funcionamiento del adaptador físico, a un error en la suma de comprobación, entre otras causas. Puede ejecutar la utilidad `pktcap-uw` para examinar en qué lugar se descartan los paquetes y el motivo del descarte.

Procedimiento

1 En ESXi Shell del host, ejecute el comando `pktcap-uw --capture Drop` con opciones para supervisar paquetes en un punto particular, filtrar paquetes capturados y guardar el resultado en un archivo.

```
pktcap-uw --capture Drop [filter_options] [--outfile pcap_file_path [--ng]] [--count
number_of_packets]
```

donde los corchetes ([]) encierran las opciones del comando `pktcap-uw--capture Drop` y las barras verticales | representan valores alternativos.

a Utilice *filter_options* para filtrar paquetes según la dirección de origen y destino, identificador de VLAN, identificador de VXLAN, protocolo de Capa 3 y puerto TCP.

   Por ejemplo, para supervisar paquetes de un sistema de origen con la dirección IP 192.168.25.113, utilice la opción de filtro `--srcip 192.168.25.113`.

b Utilice las opciones para guardar el contenido de cada paquete o el contenido de una cantidad limitada de paquetes en un archivo `.pcap` o `.pcapng`.

   - Para guardar paquetes en un archivo `.pcap`, utilice la opción `--outfile`.
   - Para guardar los paquetes en un archivo `.pcapng`, utilice las opciones `--ng` y `--outfile`.

   Puede abrir el archivo en una herramienta de análisis de red como Wireshark.

   De forma predeterminada, la utilidad `pktcap-uw` guarda los archivos de paquete en la carpeta raíz del sistema de archivos de ESXi.

   Nota Puede ver el motivo y el lugar de descarte del paquete únicamente cuando se capturan los paquetes en la salida de la consola. La utilidad `pktcap-uw` guarda únicamente el contenido de los paquetes en el archivo `.pcap` o `.pcapng`.

c Utilice la opción `--count` para supervisar solo una cantidad de paquetes.

2 Si no limitó la cantidad de paquetes con la opción `--count`, presione Ctrl+C para dejar de capturar o rastrear paquetes.

Resultados

Además del contenido de los paquetes descartados, la salida de la utilidad `pktcap-uw` muestra el motivo del descarte y la función de la pila de red que controló el paquete por última vez.

Pasos siguientes

Si el contenido del paquete se guarda en un archivo, copie el archivo del host ESXi al sistema que ejecuta una herramienta de análisis gráfico, como Wireshark, y ábralo en la herramienta para examinar los detalles del paquete.

Capturar paquetes en el nivel DVFilter

Examine cómo cambian los paquetes al pasar a través de vSphere Network Appliance (DVFilter).

Los DVFilters son agentes que residen en el flujo entre un adaptador de máquina virtual y un conmutador virtual. Su función es interceptar paquetes para proteger las máquinas virtuales contra ataques de seguridad y tráfico no deseado.

Procedimiento

1 (opcional) Para encontrar el nombre del DVFilter que desea supervisar, en ESXi Shell ejecute el comando `summarize-dvfilter`.

La salida del comando contiene los agentes de ruta de acceso rápida y lenta de los DVFilters implementados en el host.

2 Ejecute la utilidad `pktcap-uw` con el argumento `--dvfilter`*`dvfilter_name`* y con opciones para supervisar los paquetes en un punto específico, filtrar los paquetes capturados y guardar los resultados en un archivo.

```
            pktcap-uw
            --dvFilter
            dvfilter_name
            --capture PreDVFilter|PostDVFilter [filter_options] [--outfilepcap_file_path
[--ng]] [--countnumber_of_packets]
```

donde los corchetes [] demarcan los elementos opcionales del comando `pktcap-uw--dvFilter vmnicX` y las barras verticales | representan valores alternativos.

a Use la opción `--capture` para supervisar los paquetes antes o después de que los intercepte el DVFilter.

Comando opción pktcap-uw	Objetivo
--capture PreDVFilter	Se capturan los paquetes antes de que entren en el DVFilter.
--capture PostDVFilter	Se capturan los paquetes después de que entren en el DVFilter.

b Utilice *filter_ options* para filtrar paquetes según la dirección de origen y destino, identificador de VLAN, identificador de VXLAN, protocolo de Capa 3 y puerto TCP.

Por ejemplo, para supervisar paquetes de un sistema de origen con la dirección IP 192.168.25.113, utilice la opción de filtro `--srcip 192.168.25.113`.

c Utilice las opciones para guardar el contenido de cada paquete o el contenido de una cantidad limitada de paquetes en un archivo `.pcap` o `.pcapng`.

- Para guardar paquetes en un archivo `.pcap`, utilice la opción `--outfile`.
- Para guardar los paquetes en un archivo `.pcapng`, utilice las opciones `--ng` y `--outfile`.

Puede abrir el archivo en una herramienta de análisis de red como Wireshark.

De forma predeterminada, la utilidad `pktcap-uw` guarda los archivos de paquete en la carpeta raíz del sistema de archivos de ESXi.

d Utilice la opción `--count` para supervisar solo una cantidad de paquetes.

3 Si no limitó la cantidad de paquetes con la opción `--count`, presione Ctrl+C para dejar de capturar o rastrear paquetes.

Pasos siguientes

Si el contenido del paquete se guarda en un archivo, copie el archivo del host ESXi al sistema que ejecuta una herramienta de análisis gráfico, como Wireshark, y ábralo en la herramienta para examinar los detalles del paquete.

Usar los puntos de captura de la utilidad pktcap-uw

Se pueden utilizar los puntos de captura de la utilidad `pktcap-uw` para supervisar los paquetes cuando una función los controla en un lugar determinado de la pila de red de un host.

Descripción general de los puntos de captura

Un punto de captura en la utilidad `pktcap-uw` representa un lugar en la ruta de acceso entre, por un lado, un conmutador virtual y, por el otro, un adaptador físico, adaptador VMkernel o adaptador de máquina virtual.

Se pueden utilizar ciertos puntos de captura combinados con una opción de adaptador. Por ejemplo, utilice el punto UplinkRcv para capturar el tráfico de vínculo superior. Se pueden utilizar otros puntos de manera independiente. Por ejemplo, utilice el punto de descarte para inspeccionar todos los paquetes descartados.

Nota Ciertos puntos de captura de la utilidad `pktcap-uw` están diseñados para el uso interno de VMware únicamente y deben ser utilizados solo bajo la supervisión del equipo de soporte técnico de VMware. Estos puntos de captura no se describen en la guía *Redes de vSphere*.

Opción para utilizar puntos de captura en la utilidad pktcap-uw

Para examinar el estado o el contenido de un paquete en un punto de captura, agregue la opción `--capture`*capture_point* a la utilidad `pktcap-uw`.

Seleccionar un punto de captura de manera automática

En el caso del tráfico relacionado con un adaptador físico, VMkernel o VMXNET3, al combinar las opciones `--dir` y `--stage`, se puede seleccionar automáticamente un punto de captura y cambiar entre uno y otro a fin de examinar cómo cambia un paquete antes y después de un punto.

Puntos de captura de la utilidad pktcap-uw

La utilidad `pktcap-uw` admite puntos de captura que se pueden utilizar solamente cuando se supervisa el tráfico de una máquina virtual, un vínculo superior o una VMkernel, y captura puntos que representan ubicaciones especiales en la pila que no están relacionados con el tipo de adaptador.

Puntos de captura relevantes al tráfico del adaptador físico

El comando `pktcap-uw --uplink vmnic`*X* admite puntos de captura para las funciones que manejan el tráfico en una ubicación y una dirección específicas en la ruta de acceso entre el adaptador físico y el conmutador virtual.

Punto de captura	Descripción
UplinkRcv	Función que recibe los paquetes desde el adaptador físico.
UplinkSnd	Función que envía paquetes al adaptador físico.
PortInput	Función que pasa una lista de paquetes de UplinkRcv a un puerto del conmutador virtual.
PortOutput	Función que pasa una lista de paquetes de un puerto en el conmutador virtual al punto UplinkSnd.

Puntos de captura relevantes al tráfico de la máquina virtual

El comando `pktcap-uw --switchport` *`vmxnet3_port_ID`* admite puntos de captura para las funciones que manejan paquetes de tráfico en una ubicación y una dirección específicas en la ruta de acceso entre un adaptador VMXNET3 y un conmutador virtual.

Punto de captura	Descripción
VnicRx	Función en el back-end de NIC de la máquina virtual que recibe paquetes del conmutador virtual.
VnicTx	Función en el back-end de NIC de la máquina virtual que envía paquetes de la máquina virtual al conmutador virtual.
PortOutput	Función que pasa una lista de paquetes desde un puerto del conmutador virtual hasta Vmxnet3Rx.
PortInput	Función que pasa una lista de paquetes desde Vmxnet3Tx hasta un puerto del conmutador virtual. Punto de captura predeterminado para el tráfico relacionado con un adaptador VMXNET3.

Puntos de captura relevantes para el tráfico del adaptador VMkernel

Los comandos `pktcap-uw --vmk vmk`*`X`* y `pktcap-uw --switchport` *vmkernel_adapter_port_ID* admiten puntos de captura que representan funciones en una ubicación y una dirección específicas en la ruta de acceso entre un adaptador VMkernel y un conmutador virtual.

Punto de captura	Descripción
PortOutput	Función que pasa una lista de paquetes desde un puerto en el conmutador virtual hasta el adaptador VMkernel.
PortInput	Función que pasa una lista de paquetes desde el adaptador VMkernel hasta un puerto del conmutador virtual. Punto de captura predeterminado para el tráfico relacionado con un adaptador VMkernel.

Puntos de captura relevantes para filtros virtuales distribuidos

El comando `pktcap-uw --dvfilter` *`divfilter_name`* requiere un punto de captura que indica si se deben capturar paquetes cuando entran en DVFilter o cuando salen de él.

Punto de captura	Descripción
PreDVFilter	Punto anterior a que un DVFilter intercepta un paquete.
PostDVFilter	Punto posterior al que un DVFilter intercepta un paquete.

Puntos de captura independientes

Ciertos puntos de captura se asignan directamente a la pila de red en lugar de a un adaptador físico, VMkernel o VMXNET3.

Punto de captura	Descripción
Descarte	Captura paquetes descartados y muestra la ubicación donde se producen los descartes.
TcpipDispatch	Captura paquetes en la función que envía tráfico a la pila de TCP/IP del VMkernel desde el conmutador virtual, y a la inversa.
PktFree	Captura paquetes justo antes de que sean liberados.
VdrRxLeaf	Captura paquetes en la cadena de E/S de la hoja de recepción de un enrutador dinámico en VMware NSX. Utilice este punto de captura junto con la opción `--lifID`.
VdrRxTerminal	Captura paquetes en la cadena de E/S del terminal de recepción de un enrutador dinámico en VMware NSX. Utilice este punto de captura junto con la opción `--lifID`.
VdrTxLeaf	Captura paquetes en la cadena de E/S de la hoja de transmisión de un enrutador dinámico en VMware NSX. Utilice este punto de captura junto con la opción `--lifID`.
VdrTxTerminal	Captura paquetes en la cadena de E/S del terminal de transmisión de un enrutador dinámico en VMware NSX. Utilice este punto de captura junto con la opción `--lifID`.

Para obtener información sobre los enrutadores dinámicos, consulte la documentación de *VMware NSX*.

Lista de los puntos de captura de la utilidad pktcap-uw

Vea todos los puntos de captura de la utilidad `pktcap-uw` para encontrar el nombre del punto de captura que permite controlar el tráfico en un determinado lugar de la pila de red en el host ESXi.

Para obtener información sobre los puntos de captura de la utilidad `pktcap-uw`, consulte Puntos de captura de la utilidad pktcap-uw.

Procedimiento

- En la instancia de ESXi Shell conectada al host, ejecute el comando `pktcap-uw -A` para ver todos los puntos de captura que admite la utilidad `pktcap-uw`.

Rastrear paquetes mediante la utilidad pktcap-uw

Use la utilidad `pktcap-uw` para rastrear la ruta que siguen los paquetes en la pila de red para un análisis de latencia y para encontrar el punto donde se daña o se descarta un paquete.

La utilidad `pktcap-uw` muestra la ruta de acceso de los paquetes y la marca de tiempo que indica en qué momento el paquete es procesado por la función de redes de ESXi. La utilidad informa la ruta de acceso de un paquete inmediatamente antes de que salga de la pila.

Para ver la información completa de la ruta de acceso de un paquete, debe imprimir el resultado de la utilidad `pktcap-uw` en la salida de la consola o guardarlo en un archivo PCAPNG.

Procedimiento

1 En ESXi Shell para el host, ejecute el comando `pktcap-uw--trace` con opciones para filtrar los paquetes rastreados, guardar el resultado en un archivo y limitar la cantidad de paquetes rastreados.

```
            pktcap-uw
            --trace [filter_options] [--outfilepcap_file_path [--ng]]
[--countnumber_of_packets]
```

donde los corchetes [] demarcan los elementos opcionales del comando `pktcap-uw --trace` y las barras verticales | representan valores alternativos.

a Utilice *filter_ options* para filtrar paquetes según la dirección de origen y destino, identificador de VLAN, identificador de VXLAN, protocolo de Capa 3 y puerto TCP.

Por ejemplo, para supervisar paquetes de un sistema de origen con la dirección IP 192.168.25.113, utilice la opción de filtro `--srcip 192.168.25.113`.

b Utilice las opciones para guardar el contenido de cada paquete o el contenido de una cantidad limitada de paquetes en un archivo `.pcap` o `.pcapng`.

- Para guardar paquetes en un archivo `.pcap`, utilice la opción `--outfile`.
- Para guardar los paquetes en un archivo `.pcapng`, utilice las opciones `--ng` y `--outfile`.

Puede abrir el archivo en una herramienta de análisis de red como Wireshark.

De forma predeterminada, la utilidad `pktcap-uw` guarda los archivos de paquete en la carpeta raíz del sistema de archivos de ESXi.

Nota Un archivo `.pcap` incluye únicamente el contenido de los paquetes rastreados. Para recopilar las rutas de acceso de los paquetes, además del contenido, guarde la salida en un archivo `.pcapng`.

c Utilice la opción `--count` para supervisar solo una cantidad de paquetes.

2 Si no limitó la cantidad de paquetes con la opción `--count`, presione Ctrl+C para dejar de capturar o rastrear paquetes.

Pasos siguientes

Si el contenido del paquete se guarda en un archivo, copie el archivo del host ESXi al sistema que ejecuta una herramienta de análisis gráfico, como Wireshark, y ábralo en la herramienta para examinar los detalles del paquete.

Configurar opciones de NetFlow para vSphere Distributed Switch

Para analizar el tráfico IP de máquina virtual que pasa por vSphere Distributed Switch, envíe informes a un recopilador de NetFlow.

A partir de la versión 5.1 de vSphere Distributed Switch se admite IPFIX (NetFlow versión 10).

Procedimiento

1 En vSphere Web Client, desplácese hasta el conmutador distribuido.

2 En el menú **Acciones**, seleccione **Configuración > Editar NetFlow**.

3 Complete los campos **Dirección IP del recopilador** y **Puerto del recopilador** del recopilador de NetFlow.

   Puede establecer contacto con el recopilador de NetFlow a través de una dirección IPv4 o IPv6.

4 Establezca un valor de **Identificador de dominio de observación** que identifique la información relacionada con el conmutador.

5 Para ver la información desde el conmutador distribuido en el recopilador de NetFlow bajo un mismo dispositivo de red en lugar de bajo diferentes dispositivos para cada host del conmutador, escriba una dirección IPv4 en el cuadro de texto **Dirección IP del conmutador**.

6 (opcional) En los cuadros de texto **Tiempo de espera de exportación de flujo activo** y **Tiempo de espera de exportación de flujo inactivo**, establezca el tiempo, en segundos, que se esperará para enviar información a partir del inicio del flujo.

7 (opcional) Para modificar la proporción de datos recopilada por el conmutador, configure el valor de **Frecuencia de muestreo**.

   La frecuencia de muestreo representa la cantidad de paquetes que NetFlow descarta por cada paquete que recopila. Una frecuencia de muestreo de *x* le indica a NetFlow que descarte paquetes según una relación de las variables *collected packets*:*dropped packets* de 1:*x*. Si la frecuencia es 0, NetFlow toma muestras de todos los paquetes, es decir, no descarta ningún paquete por cada uno que recopila. Si la frecuencia es 1, NetFlow toma un paquete para muestreo y descarta el siguiente, y así sucesivamente.

8 (opcional) Para recopilar datos sobre la actividad de red entre máquinas virtuales en el mismo host, habilite **Solo flujos de procesos internos**.

   Recopile los flujos internos únicamente si NetFlow está habilitado en el dispositivo de red físico para que no se envíe información duplicada desde el conmutador distribuido y el dispositivo de red físico.

9 Haga clic en **Aceptar**.

Pasos siguientes

Habilite los informes de NetFlow para el tráfico desde las máquinas virtuales conectadas a un grupo de puertos distribuidos o un puerto. Consulte Habilitar o deshabilitar la supervisión de NetFlow en un puerto distribuido o en un grupo de puertos distribuidos.

Trabajar con una creación de reflejo del puerto

La creación de reflejo del puerto permite reflejar el tráfico de un puerto distribuido a otros puertos distribuidos o a puertos específicos del conmutador físico.

La creación de reflejo del puerto se utiliza en un conmutador para enviar una copia de los paquetes vistos en un puerto de conmutador (o de una VLAN completa) hacia una conexión de supervisión en otro puerto del conmutador. La creación de reflejo del puerto se utiliza para analizar y depurar datos o para diagnosticar errores en una red.

Compatibilidad de la versión de creación de reflejo del puerto

Ciertas funcionalidades de creación de reflejo del puerto en vSphere 5.1 y posteriores dependen de la versión de vCenter Server, del conmutador distribuido de vSphere y del host que utilice, y de la forma en que utilice estos aspectos de vSphere de forma conjunta.

Tabla 14-5. Compatibilidad de la creación de reflejo del puerto

Versión de vCenter Server	Versión de vSphere Distributed Switch	Versión del host	Funcionalidad de la creación de reflejo del puerto de vSphere 5.1
vSphere 5.1 y posteriores	vSphere 5.1 y posteriores	vSphere 5.1 y posteriores	La creación de reflejo del puerto de vSphere 5.1 está disponible para utilizarse. Las características de creación de reflejo del puerto para vSphere 5.0 y anteriores no están disponibles.
vSphere 5.1 y posteriores	vSphere 5.1 y posteriores	vSphere 5.0 y anteriores	Los hosts de vSphere 5.0 y anteriores pueden agregarse a vSphere 5.1 vCenter Server, pero no pueden agregarse a conmutadores distribuidos versión 5.1 y posteriores.
vSphere 5.1 y posteriores	vSphere 5.0	vSphere 5.0	vSpherevCenter Server versión 5.1 y posteriores pueden configurar la creación de reflejo del puerto en un conmutador distribuido de vSphere 5.0.

Tabla 14-5. Compatibilidad de la creación de reflejo del puerto (continuación)

Versión de vCenter Server	Versión de vSphere Distributed Switch	Versión del host	Funcionalidad de la creación de reflejo del puerto de vSphere 5.1
vSphere 5.1 y posteriores	vSphere 5.0	vSphere 5.1 y posteriores	Los hosts que ejecutan vSphere 5.1 pueden agregarse a conmutadores distribuidos de vSphere 5.0 y admitir la creación de reflejo del puerto en vSphere 5.0.
vSphere 5.1 y posteriores	Antes de vSphere 5.0	vSphere 5.5 y anteriores	No se admite la creación de reflejo del puerto.
vSphere 5.0 y anteriores	vSphere 5.0 y anteriores	vSphere 5.1	Un host de vSphere 5.1 no puede agregarse a vCenter Server 5.0 y anteriores.

Si utiliza un perfil de host con la configuración de creación de reflejo del puerto, el perfil del host debe adaptarse a la nueva versión de creación de reflejo del puerto en vSphere 5.1 y posteriores.

Interoperabilidad de creación de reflejo del puerto

Hay algunos problemas de interoperabilidad que se deben tener en cuenta al utilizar la creación de reflejo del puerto de vSphere con otras características de vSphere.

vMotion

vMotion funciona de manera diferente según qué sesión de creación de reflejo del puerto de vSphere se seleccione. Durante vMotion, una ruta de acceso de reflejo podría ser temporalmente no válida, pero se restaura cuando se completa vMotion.

Tabla 14-6. Interoperabilidad de vMotion con la creación de reflejo del puerto

Tipo de sesión de creación de reflejo del puerto	Origen y destino	Interoperable con vMotion	Funcionalidad
Creación de reflejo del puerto distribuido	Origen y destino de puertos distribuidos sin vínculos superiores	Sí	La creación de reflejo del puerto entre puertos distribuidos solo puede ser local. Si el origen y el destino están en hosts diferentes debido a vMotion, la creación de reflejo entre ellos no funciona. Sin embargo, si el origen y el destino se mueven al mismo host, la creación de reflejo del puerto funciona.
Origen de creación de reflejo remoto	Origen de puerto distribuido sin vínculo superior	Sí	Cuando un puerto distribuido de origen se mueve del host A al B, la ruta de acceso de creación de reflejo original del puerto de origen al vínculo superior de A se elimina en A, y se crea una nueva ruta de acceso de creación de reflejo desde el puerto de origen hasta el vínculo superior de B. El nombre del vínculo superior especificado en la sesión determina el vínculo superior que se va a utilizar.
	Destinos de puerto de vínculo superior	No	vMotion no puede mover los vínculos superiores.
Destino de creación de reflejo remoto	Origen de VLAN	No	
	Destino de puerto distribuido sin vínculo superior	Sí	Cuando un puerto de destino distribuido se mueve del host A al B, todas las rutas de acceso de creación de reflejo originales de las VLAN de origen al puerto de destino también se mueven de A a B.

Tabla 14-6. Interoperabilidad de vMotion con la creación de reflejo del puerto (continuación)

Tipo de sesión de creación de reflejo del puerto	Origen y destino	Interoperable con vMotion	Funcionalidad
Origen de creación de reflejo remoto encapsulado (L3)	Origen de puerto distribuido sin vínculo superior	Sí	Cuando un puerto distribuido de origen se mueve del host A al B, todas las rutas de acceso originales de creación de reflejo del puerto de origen a las IP de destino se mueven de A a B.
	Destino de IP	No	
Creación de reflejo del puerto distribuido (heredado)	Origen de IP	No	
	Destino de puerto distribuido sin vínculo superior	No	Cuando un puerto distribuido de destino se mueve del host A al B, todas las rutas de acceso de creación de reflejo originales de las IP de origen al puerto de destino no son válidas, ya que el origen de la sesión de creación de reflejo del puerto aún sigue viendo el destino en A.

TSO y LRO

La descarga de segmentación de TCP (TSO) y la descarga de recepción grande (LRO) pueden causar que la cantidad de paquetes de creación de reflejo no sea igual a la cantidad de paquetes reflejados.

Cuando se habilita TSO en una vNIC, la vNIC puede enviar un paquete grande a un conmutador distribuido. Cuando se habilita LRO en una vNIC, los paquetes pequeños que se le envían pueden fusionarse en uno grande.

Origen	Destino	Descripción
TSO	LRO	Los paquetes de la vNIC de origen pueden ser grandes. Si su tamaño es mayor al de la limitación de LRO de la vNIC de destino, se dividirán.
TSO	Cualquier destino	Los paquetes de la vNIC de origen pueden ser grandes y se dividen en paquetes estándar en la vNIC de destino.
Cualquier origen	LRO	Los paquetes de la vNIC de origen son estándar y pueden fusionarse en paquetes más grandes en la vNIC de destino.

Crear una sesión de creación de reflejo del puerto

Para crear una sesión de creación de reflejo del puerto, use vSphere Web Client para reflejar el tráfico de vSphere Distributed Switch a puertos, vínculos superiores y direcciones IP remotas.

Requisitos previos

Compruebe que la versión de vSphere Distributed Switch sea 5.0.0 o posterior.

Procedimiento

1 Seleccionar tipo de sesión de creación de reflejo del puerto

Para iniciar una sesión de creación de reflejo del puerto, debe especificar el tipo de sesión.

2 Especificar el nombre de creación de reflejo del puerto y los detalles de sesión

Para seguir creando una sesión de reflejo del puerto, especifique el nombre, la descripción y los detalles de la sesión para la nueva sesión de creación de reflejo del puerto.

3 Seleccionar orígenes de creación de reflejo del puerto

Para seguir configurando una sesión de creación de reflejo del puerto, seleccione los orígenes y la dirección del tráfico de la nueva sesión de creación de reflejo del puerto.

4 Seleccionar destinos de creación de reflejo del puerto y comprobación de la configuración

Para finalizar la creación de una sesión de reflejo del puerto, seleccione puertos o vínculos superiores como destinos de la sesión de creación de reflejo del puerto.

Seleccionar tipo de sesión de creación de reflejo del puerto

Para iniciar una sesión de creación de reflejo del puerto, debe especificar el tipo de sesión.

Procedimiento

1 Desplácese hasta un conmutador distribuido en el navegador de vSphere Web Client.

2 Haga clic en la pestaña **Configurar** y expanda **Opciones de configuración**.

3 Seleccione la opción **Creación de reflejo del puerto** y haga clic en **Nuevo**.

4 Seleccione el tipo de sesión de creación de reflejo del puerto.

Opción	Descripción
Creación de reflejo del puerto distribuido	Refleja los paquetes de varios puertos distribuidos a otros puertos distribuidos en el mismo host. Si el origen y el destino están en diferentes hosts, este tipo de sesión no funciona.
Origen de creación de reflejo remoto	Refleja los paquetes de varios puertos distribuidos a puertos de vínculo superior específicos en el host correspondiente.
Destino de creación de reflejo remoto	Refleja los paquetes de varias VLAN a puertos distribuidos.
Origen de creación de reflejo remoto encapsulado (L3)	Refleja los paquetes de varios puertos distribuidos en las direcciones IP de un agente remoto. El tráfico de la máquina virtual se refleja en un destino físico remoto a través de un túnel IP.
Creación de reflejo del puerto distribuido (heredado)	Refleja los paquetes de varios puertos distribuidos a varios puertos distribuidos o puertos de vínculo superior en el host correspondiente.

5 Haga clic en **Siguiente**.

Especificar el nombre de creación de reflejo del puerto y los detalles de sesión

Para seguir creando una sesión de reflejo del puerto, especifique el nombre, la descripción y los detalles de la sesión para la nueva sesión de creación de reflejo del puerto.

Procedimiento

1 Establezca las propiedades de la sesión. Las opciones disponibles para la configuración dependen del tipo de sesión seleccionado.

Opción	Descripción
Nombre	Puede escribir un nombre exclusivo para la sesión de creación de reflejo del puerto o aceptar el nombre de sesión generado automáticamente.
Estado	Utilice el menú desplegable para habilitar o deshabilitar la sesión.
Tipo de sesión	Muestra el tipo de sesión seleccionado.
E/S normal en puertos de destino	Use el menú desplegable para permitir o no la E/S normal en los puertos de destino. Esta propiedad solamente está disponible para los destinos de vínculo superior y de puerto distribuido. Si deshabilita esta opción, se permite la salida del tráfico reflejado en los puertos de destino, pero no se permite la entrada del tráfico.
Longitud de paquetes reflejados (bytes)	Use esta casilla para establecer la longitud de los paquetes reflejados en bytes. Esta opción limita el tamaño de las tramas que se reflejan. Si se selecciona esta opción, los caracteres de todas las tramas reflejadas se truncan al alcanzar la longitud especificada.
Frecuencia de muestreo	Seleccione la frecuencia con la que se obtienen las muestras de paquetes. Esta opción está habilitada de forma predeterminada para todas las sesiones de creación de reflejo del puerto, excepto para las sesiones heredadas.
Descripción	Tiene la opción de escribir una descripción de la configuración de sesión de creación de reflejo del puerto.

2 Haga clic en **Siguiente**.

Seleccionar orígenes de creación de reflejo del puerto

Para seguir configurando una sesión de creación de reflejo del puerto, seleccione los orígenes y la dirección del tráfico de la nueva sesión de creación de reflejo del puerto.

Puede crear una sesión de creación de reflejo del puerto sin configurar el origen y los destinos. Cuando no se establece un origen ni un destino, la sesión de creación de reflejo del puerto se crea sin ruta de reflejo. De esta forma, es posible crear una sesión de creación de reflejo del puerto con las propiedades establecidas correspondientes. Una vez que se establecen las propiedades, puede editar la sesión de creación de reflejo del puerto para agregar información sobre el origen y el destino.

Nota Tenga en cuenta las siguientes limitaciones al seleccionar los orígenes de creación de reflejo del puerto.

- Un puerto de reflejo de origen no se puede utilizar en más de una sesión de reflejo.
- Un puerto no se puede utilizar como origen de reflejo y destino de reflejo en la misma sesión de reflejo o en sesiones diferentes al mismo tiempo.

Procedimiento

1 Seleccione el origen del tráfico que se reflejará y la dirección del tráfico.

Las opciones de configuración disponibles varían en función de la sesión de creación de reflejo del puerto seleccionada.

Opción	Descripción
Agregar puertos existentes de una lista	Haga clic en **Seleccionar puertos distribuidos**. Se muestra un cuadro de diálogo con una lista de los puertos existentes. Active la casilla que aparece junto al puerto distribuido y haga clic en **Aceptar**. Puede elegir más de un puerto distribuido.
Agregar puertos existentes por número de puerto	Haga clic en **Agregar puertos distribuidos**, escriba el número de puerto y haga clic en **Aceptar**.
Establecer dirección del tráfico	Después de agregar los puertos, seleccione un puerto en la lista y haga clic en el botón de ingreso, egreso o ingreso/egreso. La opción se muestra en la columna Dirección del tráfico.
Especificar VLAN de origen	Si seleccionó el tipo de sesión Destino de reflejo remoto, debe especificar la VLAN de origen. Haga clic en **Agregar** para agregar un ID de VLAN. Para modificar el identificador puede usar las flechas hacia arriba y hacia abajo, o bien hacer clic en el campo e introducir manualmente el identificador de VLAN.

2 Haga clic en **Siguiente**.

Seleccionar destinos de creación de reflejo del puerto y comprobación de la configuración

Para finalizar la creación de una sesión de reflejo del puerto, seleccione puertos o vínculos superiores como destinos de la sesión de creación de reflejo del puerto.

Puede crear una sesión de creación de reflejo del puerto sin configurar el origen y los destinos. Cuando no se establece un origen ni un destino, la sesión de creación de reflejo del puerto se crea sin ruta de reflejo. De esta forma, es posible crear una sesión de creación de reflejo del puerto con las propiedades establecidas correspondientes. Una vez que se establecen las propiedades, puede editar la sesión de creación de reflejo del puerto para agregar información sobre el origen y el destino.

La creación de reflejo del puerto se compara con la directiva de reenvío de VLAN. Si la VLAN de las tramas originales no es igual al puerto de destino o no está enlazada troncalmente por él, las tramas no se reflejan.

Procedimiento

1 Seleccione el destino de la sesión de creación de reflejo del puerto.

   Las opciones disponibles dependen del tipo de sesión que elija.

Opción	Descripción
Seleccionar un puerto distribuido de destino	Haga clic en **Seleccionar puertos distribuidos** de una lista o haga clic en **Agregar puertos distribuidos** para agregar puertos por número de puerto. Puede agregar más de un puerto distribuido.
Seleccionar un vínculo superior	Seleccione un vínculo superior disponible de la lista y haga clic en **Agregar** para agregarlo a una sesión de creación de reflejo del puerto. Puede seleccionar más de un vínculo superior.
Seleccionar puertos o vínculos superiores	Haga clic en **Seleccionar puertos distribuidos** de una lista o haga clic en **Agregar puertos distribuidos** para agregar puertos por número de puerto. Puede agregar más de un puerto distribuido. Haga clic en **Agregar vínculos superiores** para agregar vínculos superiores como destino. Seleccione vínculos superiores de la lista y haga clic **Aceptar**.
Especificar dirección IP	Haga clic en **Agregar**. Se crea una nueva entrada de lista. Seleccione la entrada y haga clic en **Editar** para introducir la dirección IP o haga clic directamente en el campo Dirección IP y escriba la dirección IP. Si la dirección IP no es válida, aparece una advertencia.

2 Haga clic en **Siguiente**.

3 Revise la información que introdujo para la sesión de creación de reflejo del puerto en la página **Listo para finalizar**.

4 (opcional) Utilice el botón **Atrás** para editar la información.

5 Haga clic en **Finalizar**.

Resultados

La nueva sesión de creación de reflejo del puerto aparece en la sección Creación de reflejo del puerto de la pestaña **Configuración**.

Ver los detalles de la sesión de creación de reflejo del puerto

Es posible ver los detalles de la sesión de creación de reflejo del puerto, incluido el estado, los orígenes y los destinos.

Procedimiento

1 En vSphere Web Client, desplácese hasta el conmutador distribuido.

2 En la pestaña **Configurar**, expanda **Configuración** y haga clic en **Creación de reflejo del puerto**.

3 Seleccione una sesión de creación de reflejo del puerto en la lista para mostrar información detallada en la parte inferior de la pantalla. En las pestañas, puede revisar los detalles de la configuración.

4 (opcional) Haga clic en **Nueva** para agregar una nueva sesión de creación de reflejo del puerto.

5 (opcional) Haga clic en **Editar** para editar los detalles de la sesión de creación de reflejo del puerto seleccionada.

6 (opcional) Haga clic en **Quitar** para eliminar la sesión de creación de reflejo del puerto seleccionada.

Editar detalles, orígenes y destinos de la sesión de creación de reflejo del puerto

Puede editar los detalles de una sesión de creación de reflejo del puerto, como el nombre, la descripción, el estado, los orígenes y los destinos.

Procedimiento

1 En vSphere Web Client, desplácese hasta el conmutador distribuido.

2 En la pestaña **Configurar**, expanda **Configuración** y haga clic en **Creación de reflejo del puerto**.

3 Seleccione una sesión de creación de reflejo del puerto de la lista y haga clic en **Editar**.

4 En la página **Propiedades**, modifique las propiedades de la sesión.

Las opciones de configuración disponibles varían en función de la sesión de creación de reflejo del puerto que se está editando.

Opción	Descripción
Nombre	Puede escribir un nombre exclusivo para la sesión de creación de reflejo del puerto o aceptar el nombre de sesión generado automáticamente.
Estado	Utilice el menú desplegable para habilitar o deshabilitar la sesión.

Opción	Descripción
E/S normal en puertos de destino	Use el menú desplegable para permitir o no la E/S normal en los puertos de destino. Esta propiedad solamente está disponible para los destinos de vínculo superior y de puerto distribuido. Si no selecciona esta opción, se permite que el tráfico reflejado salga de los puertos de destino, pero no se permite tráfico entrante.
Identificador de VLAN de encapsulación	Escriba un identificador de VLAN válido en el campo. Esta información es necesaria para las sesiones de creación de reflejo del puerto Origen de reflejo remoto. Active la casilla que se muestra junto a **Conservar VLAN original** para crear un identificador de VLAN que encapsule todas las tramas de los puertos de destino. Si las tramas originales tienen una VLAN y no se selecciona esta opción, la VLAN de encapsulación sustituye a la VLAN original.
Longitud de paquetes reflejados (bytes)	Use esta casilla para establecer la longitud de los paquetes reflejados en bytes. Esta opción limita el tamaño de las tramas que se reflejan. Si se selecciona esta opción, los caracteres de todas las tramas reflejadas se truncan al alcanzar la longitud especificada.
Descripción	Tiene la opción de escribir una descripción de la configuración de sesión de creación de reflejo del puerto.

5 En la página **Orígenes**, modifique los orígenes de la sesión de creación de reflejo del puerto.

Las opciones de configuración disponibles varían en función de la sesión de creación de reflejo del puerto que se está editando.

Opción	Descripción
Agregar puertos existentes de una lista	Haga clic en el botón **Seleccionar puertos distribuidos...**. Se abre un cuadro de diálogo con una lista de los puertos existentes. Active la casilla que aparece junto al puerto distribuido y haga clic en **Aceptar**. Puede elegir más de un puerto distribuido.
Agregar puertos existentes por número de puerto	Haga clic en **Agregar puertos distribuidos**, escriba el número de puerto y haga clic en **Aceptar**.
Establecer dirección del tráfico	Después de agregar los puertos, seleccione un puerto en la lista y haga clic en el botón de ingreso, egreso o ingreso/egreso. La opción se muestra en la columna Dirección del tráfico.
Especificar VLAN de origen	Si seleccionó el tipo de sesión Destino de reflejo remoto, debe especificar la VLAN de origen. Haga clic en el botón **Agregar** para agregar un identificador de VLAN. Para modificar el identificador puede usar las flechas hacia arriba y hacia abajo, o bien hacer clic en el campo e introducir manualmente el identificador de VLAN.

6 En la sección **Destinos**, modifique los destinos de la sesión de creación de reflejo del puerto.

Las opciones de configuración disponibles varían en función de la sesión de creación de reflejo del puerto que se está editando.

Opción	Descripción
Seleccionar un puerto distribuido de destino	Haga clic en el botón **Seleccionar puertos distribuidos** para seleccionar puertos de una lista o haga clic en el botón **Agregar puertos distribuidos** para agregar puertos por número de puerto. Puede agregar más de un puerto distribuido.
Seleccionar un vínculo superior	Seleccione un vínculo superior disponible de la lista y haga clic en **Agregar >** para agregarlo a una sesión de creación de reflejo del puerto. Puede seleccionar más de un vínculo superior.
Seleccionar puertos o vínculos superiores	Haga clic en el botón **Seleccionar puertos distribuidos** para seleccionar puertos de una lista o haga clic en el botón **Agregar puertos distribuidos** para agregar puertos por número de puerto. Puede agregar más de un puerto distribuido. Haga clic en el botón **Agregar vínculos superiores...** para agregar vínculos superiores como destino. Seleccione vínculos superiores de la lista y haga clic **Aceptar**.
Especificar dirección IP	Haga clic en el botón **Agregar**. Se crea una nueva entrada de lista. Seleccione la entrada y haga clic en el botón Editar para introducir la dirección IP o haga clic directamente en el campo Dirección IP y escriba la dirección IP. Si la dirección IP no es válida, se abre un cuadro de diálogo de advertencia.

7 Haga clic en **Aceptar**.

Comprobar estado de vSphere Distributed Switch

La compatibilidad con la comprobación de estado permite identificar y solucionar los errores de configuración en una instancia de vSphere Distributed Switch.

Utilice la comprobación de estado de vSphere Distributed Switch para examinar determinados ajustes de los conmutadores físicos y distribuidos con el fin de identificar errores comunes en la configuración de redes del entorno. El intervalo predeterminado entre dos comprobaciones de estado es de 1 minuto.

Importante Utilice la comprobación de estado para solucionar problemas de red y, después de identificar y resolver el problema, deshabilítela. Después de deshabilitar la comprobación de estado de vSphere Distributed Switch, las direcciones MAC generadas caducan en el entorno de red física de acuerdo con la directiva de red. Para obtener más información, consulte el artículo de la base de conocimientos KB 2034795.

Error de configuración	Comprobación de estado	Configuración requerida en el conmutador distribuido
Los rangos del tronco de VLAN configurados en el conmutador distribuido no coinciden con los rangos troncales en el conmutador físico.	Comprueba si la configuración de VLAN en el conmutador distribuido coincide con la configuración de puerto troncal en los puertos del conmutador físico conectado.	Al menos dos NIC físicas activas
La configuración de MTU en los adaptadores de red físicos, el conmutador distribuido y los puertos del conmutador físico no coinciden.	Comprueba si la configuración de la trama gigante de MTU del puerto del conmutador de acceso físico basado en cada VLAN coincide con la configuración de MTU del conmutador distribuido de vSphere.	Al menos dos NIC físicas activas
La directiva de formación de equipos configurada en los grupos de puertos no coincide con la directiva en el canal-puerto del conmutador físico.	Comprueba si los puertos de acceso conectados del conmutador físico que participan en una instancia de EtherChannel están emparejados con los puertos distribuidos cuya directiva de formación de equipos está configurada como hash de IP.	Al menos dos NIC físicas activas y dos hosts

La comprobación de estado se limita solo al puerto del conmutador de acceso al que se conecta el vínculo superior del conmutador distribuido.

Habilitar o deshabilitar la comprobación de estado de vSphere Distributed Switch

Use la comprobación de estado de vSphere Distributed Switch para supervisar las configuraciones del conmutador distribuido e identificar y resolver los problemas de red.

La comprobación de estado de vSphere Distributed Switch permite identificar y solucionar problemas de configuración con vSphere Distributed Switch (VDS), así como las configuraciones que no coinciden entre VDS y la red física del entorno. De forma predeterminada, la comprobación de estado está desactivada. Puede habilitar la comprobación de estado para identificar y resolver los problemas de red pueda experimentar. En función de las opciones que seleccione, la comprobación de estado de vSphere Distributed Switch puede generar una cantidad significativa de direcciones MAC para probar las directivas de formación de equipos, el tamaño de MTU y la configuración de VLAN. Estas direcciones MAC generan un tráfico de red adicional, lo que puede afectar al rendimiento de la red.

Importante Utilice la comprobación de estado para solucionar problemas de red y, después de identificar y resolver el problema, deshabilítela. Después de deshabilitar la comprobación de estado de vSphere Distributed Switch, las direcciones MAC generadas caducan en el entorno de red física de acuerdo con la directiva de red. Para obtener más información, consulte el artículo de la base de conocimientos KB 2034795.

Procedimiento

1 En vSphere Web Client, desplácese hasta el conmutador distribuido.

2 En el menú **Acciones**, seleccione **Configuración > Editar comprobación de estado**.

3 Use los menús desplegables para habilitar o deshabilitar las opciones de comprobación de estado.

Opción	Descripción
VLAN y MTU	Informa el estado de los puertos de vínculo superior distribuidos y los rangos de VLAN.
Formación de equipos y conmutación por error	Comprueba si no coincide la configuración entre el host ESXi y el conmutador físico que se usa en la directiva de formación de equipos.

4 Haga clic en **Aceptar**.

Pasos siguientes

Cuando se cambia la configuración de vSphere Distributed Switch, puede ver información sobre el cambio en la pestaña **Supervisar** en vSphere Web Client. Consulte Ver estado de mantenimiento de vSphere Distributed Switch.

Ver estado de mantenimiento de vSphere Distributed Switch

Cuando se habilita la comprobación de estado en vSphere Distributed Switch, es posible ver el estado de mantenimiento de la red de los hosts conectados en vSphere Web Client.

Requisitos previos

Compruebe que la comprobación de estado de VLAN y MTU, y de la directiva de formación de equipos, estén habilitadas en vSphere Distributed Switch. Consulte Habilitar o deshabilitar la comprobación de estado de vSphere Distributed Switch.

Procedimiento

1 En vSphere Web Client, desplácese hasta el conmutador distribuido.

2 En la pestaña **Supervisar**, haga clic en **Estado**.

3 En la sección Detalles del estado de mantenimiento, examine el estado general, de VLAN, de MTU y de formación de equipos de los hosts conectados al conmutador.

Protocolo de detección de conmutadores

Los protocolos de detección de conmutadores ayudan a los administradores de vSphere a establecer qué puerto del conmutador físico se conecta a un conmutador estándar de vSphere o a un conmutador distribuido de vSphere.

vSphere 5.0, y versiones posteriores, admite los protocolos Cisco Discovery Protocol (CDP) y Link Layer Discovery Protocol (LLDP). CDP está disponible para los conmutadores estándar de vSphere y los conmutadores distribuidos de vSphere conectados a conmutadores físicos de Cisco. LLDP está disponible para los conmutadores distribuidos vSphere de la versión 5.0.0 y posteriores.

Cuando se habilita CDP o LLDP para un conmutador distribuido de vSphere o un conmutador estándar de vSphere en particular, puede ver las propiedades del conmutador físico del mismo nivel, como identificador del dispositivo, versión de software y tiempo de espera, desde vSphere Web Client.

Habilitar el protocolo Cisco Discovery Protocol en vSphere Distributed Switch

El protocolo Cisco Discovery Protocol (CDP) permite que los administradores de vSphere determinen cuál es el puerto del conmutador físico de Cisco que se conecta a vSphere Standard Switch o vSphere Distributed Switch. Cuando se habilita el CDP para vSphere Distributed Switch, se pueden ver las propiedades del conmutador de Cisco, como el identificador del dispositivo, la versión de software y el tiempo de espera.

Procedimiento

1 En vSphere Web Client, desplácese hasta el conmutador distribuido.

2 En el menú **Acciones**, seleccione **Configuración > Editar configuración**.

3 En el cuadro de diálogo Editar configuración, haga clic en **Avanzado**.

4 En la sección Protocolo de detección, seleccione **Cisco Discovery Protocol** en el menú desplegable **Tipo**.

5 En el menú desplegable **Funcionamiento**, seleccione el modo operativo de los hosts ESXi conectados al conmutador.

Opción	Descripción
Escuchar	ESXi detecta y muestra la información sobre el puerto del conmutador de Cisco asociado, pero no permite que el administrador del conmutador de Cisco vea la información sobre vSphere Distributed Switch.
Anunciar	ESXi permite que el administrador del conmutador de Cisco vea la información sobre vSphere Distributed Switch, pero no detecta ni muestra información sobre el conmutador de Cisco.
Ambas	ESXi detecta y muestra información sobre el conmutador de Cisco asociado y permite que el administrador del conmutador de Cisco vea la información sobre vSphere Distributed Switch.

6 Haga clic en **Aceptar**.

Habilitar el protocolo Link Layer Discovery Protocol en vSphere Distributed Switch

Con el protocolo Link Layer Discovery Protocol (LLDP), los administradores de vSphere pueden determinar qué puerto del conmutador físico se conecta con vSphere Distributed Switch. Cuando se habilita LLDP para un conmutador distribuido determinado, es posible ver las propiedades de un conmutador físico (como el identificador del chasis, el nombre y la descripción del sistema, y las capacidades del dispositivo) en vSphere Web Client.

Procedimiento

1. En vSphere Web Client, desplácese hasta el conmutador distribuido.
2. En el menú **Acciones**, seleccione **Configuración > Editar configuración**.
3. En el cuadro de diálogo Editar configuración, haga clic en **Avanzado**.
4. En la sección Protocolo de detección, seleccione **Protocolo de detección de nivel de vínculo** en el menú desplegable **Tipo**.
5. En el menú desplegable **Funcionamiento**, seleccione el modo operativo de los hosts ESXi conectados al conmutador.

Operación	Descripción
Escuchar	ESXi detecta y muestra la información sobre el puerto de conmutador físico asociado, pero no permite que el administrador de conmutadores vea la información sobre vSphere Distributed Switch.
Anunciar	ESXi permite que el administrador de conmutadores vea la información sobre vSphere Distributed Switch, pero no detecta ni muestra información sobre el conmutador físico.
Ambas	ESXi detecta y muestra información sobre el conmutador físico asociado y permite que el administrador de conmutadores vea la información sobre vSphere Distributed Switch.

6. Haga clic en **Aceptar**.

Ver la información del conmutador

Cuando se habilita el protocolo CDP o LLDP en el conmutador distribuido y los hosts conectados al conmutador están en el modo operativo Escucha o Ambos, es posible ver la información sobre el conmutador físico desde vSphere Web Client.

Procedimiento

1. En vSphere Web Client, desplácese hasta el host.
2. En la pestaña **Configurar**, expanda **Redes** y haga clic en **Adaptadores físicos**.
3. Seleccione un adaptador físico de la lista para ver la información detallada.

Resultados

Según cuál sea el protocolo de detección del conmutador habilitado, las propiedades del conmutador se muestran en la pestaña **CDP** o **LLDP**. Si la información está disponible en la red, en la capacidad del dispositivo del mismo nivel puede examinar las capacidades del sistema del conmutador.

Configurar los perfiles de protocolo para redes de máquinas virtuales

15

Un perfil de protocolo de red contiene un grupo de direcciones IPv4 e IPv6 que vCenter Server asigna a las vApps o las máquinas virtuales con funcionalidad vApp que están conectadas a grupos de puertos asociados con el perfil.

Los perfiles de protocolo de red también contienen configuración para la subred IP, el DNS y el servidor proxy HTTP.

Para establecer la configuración de red de las máquinas virtuales mediante el uso de perfiles de protocolo de red, realice las siguientes operaciones:

- Cree perfiles de red en el nivel de un centro de datos o un conmutador distribuido de vSphere.
- Asocie un perfil de protocolo con el grupo de puertos de una máquina virtual vApp.
- En la configuración de vApp o en las opciones de vApp de una máquina virtual, habilite la directiva de asignación de IP transitoria o estática.

Nota Si mueve una vApp o una máquina virtual que recupera su configuración de red desde un perfil de protocolo hacia otro centro de datos, al encenderlo se deberá asignar un perfil de protocolo al grupo de puertos conectado en el centro de datos de destino.

- Agregar un perfil de protocolo de red

  Un perfil de protocolo de red contiene un grupo de direcciones IPv4 e IPv6. vCenter Server asigna esos recursos a vApps o a máquinas virtuales con la funcionalidad vApp que estén conectadas a los grupos de puertos asociados con el perfil.

- Asociación de un grupo de puertos con un perfil de protocolo de red

  Para aplicar el rango de direcciones IP desde un perfil de protocolo de red a una máquina virtual que forma parte de una vApp o tiene habilitada la funcionalidad de vApp, asocie el perfil con un grupo de puertos que controle las redes de la máquina virtual.

- Configurar una máquina virtual o vApp para que utilice un perfil de protocolo de red

  Después de asociar un perfil de protocolo a un grupo de puertos de un conmutador estándar o distribuido, habilite el uso del perfil en una máquina virtual que esté conectada al grupo de puertos y que esté asociada con una vApp o tenga las opciones de vApp habilitadas.

Agregar un perfil de protocolo de red

Un perfil de protocolo de red contiene un grupo de direcciones IPv4 e IPv6. vCenter Server asigna esos recursos a vApps o a máquinas virtuales con la funcionalidad vApp que estén conectadas a los grupos de puertos asociados con el perfil.

Los perfiles de protocolo de red también contienen configuración para la subred IP, el DNS y el servidor proxy HTTP.

Nota Si traslada una vApp o una máquina virtual que recupera su configuración de red desde un perfil de protocolo a otro centro de datos, para encender la vApp o la máquina virtual debe asignar un perfil de protocolo al grupo de puertos conectado en el centro de datos de destino.

Procedimiento

1 Desplácese hasta el centro de datos asociado con la vApp y haga clic en la pestaña **Configurar**.

2 Haga clic en **Perfiles de protocolo de red**.

  Se enumeran los perfiles de protocolo de red existentes.

3 Haga clic en el icono de adición (✚) para agregar un nuevo perfil de protocolo de red.

Seleccionar la red y el nombre del perfil de protocolo de red

Asigne un nombre al perfil de protocolo de red y seleccione la red que debe utilizarlo.

Procedimiento

1 Escriba el nombre del perfil de protocolo de red.

2 Seleccione las redes que utilizan este perfil de protocolo de red.

  La red puede asociarse con un solo perfil de protocolo de red a la vez.

3 Haga clic en **Siguiente**.

Especificar la configuración de IPv4 del perfil de protocolo de red

Un perfil de protocolo de red contiene un grupo de direcciones IPv4 y IPv6 usadas por las vApps. Cuando se crea un perfil de protocolo de red, se configuran las opciones de IPv4.

Se pueden configurar los rangos de perfil de protocolo de red para IPv4, IPv6 o ambos.vCenter Server utiliza estos rangos para asignar direcciones IP de forma dinámica a las máquinas virtuales cuando una vApp está configurada para utilizar la asignación transitoria de IP.

Procedimiento

1 Introduzca los valores de **Subred IP** y **Puerta de enlace** en sus respectivos campos.

2 Seleccione **DHCP presente** para indicar que el servidor DHCP está disponible en la red.

3 Introduzca la información del servidor DNS.

Especifique los servidores mediante las direcciones IP separadas por coma, punto y coma o espacio.

4 Active la casilla **Habilitar grupo de direcciones IP** para especificar un rango para el grupo de IP.

5 Si habilita los grupos de direcciones IP, introduzca una lista de rangos de direcciones de host, separados por comas, en el campo **Rango de grupo de direcciones IP**.

El rango consiste en una dirección IP, un signo numeral (#) y un número que indique la longitud del rango.

La puerta de enlace y los rangos deben encontrarse dentro de la subred. Los rangos indicados en el campo **Rango de grupo de direcciones IP** no pueden incluir la dirección de la puerta de enlace.

Por ejemplo, **`10.20.60.4#10, 10.20.61.0#2`** indica que las direcciones IPv4 pueden encontrarse entre 10.20.60.4 y 10.20.60.13 y entre 10.20.61.0 y 10.20.61.1.

6 Haga clic en **Siguiente**.

Especificar una configuración IPv6 para el perfil de protocolo de red

Un perfil de protocolo de red contiene un grupo de direcciones IPv4 y IPv6 usadas por las vApps. Al crear un perfil de protocolo de red, se establece la configuración IPv6.

Se pueden configurar los rangos de perfil de protocolo de red para IPv4, IPv6 o ambos.vCenter Server utiliza estos rangos para asignar direcciones IP de forma dinámica a las máquinas virtuales cuando una vApp está configurada para utilizar la asignación transitoria de IP.

Procedimiento

1 Introduzca los valores de **Subred IP** y **Puerta de enlace** en sus respectivos campos.

2 Seleccione **DHCP presente** para indicar que el servidor DHCP está disponible en la red.

3 Introduzca la información del servidor DNS.

Especifique los servidores mediante las direcciones IP separadas por coma, punto y coma o espacio.

4 Active la casilla **Habilitar grupo de direcciones IP** para especificar un rango para el grupo de IP.

5 Si habilita los grupos de direcciones IP, introduzca una lista de rangos de direcciones de host, separados por comas, en el campo **Rango de grupo de direcciones IP**.

El rango consiste en una dirección IP, un signo numeral (#) y un número que indique la longitud del rango. Por ejemplo, supongamos que especifica el siguiente rango de grupos de direcciones IP:

fe80:0:0:0:2bff:fe59:5a:2b#10,fe80:0:0:0:2bff:fe59:5f:b1#2

Las direcciones se encuentran en el siguiente rango:

fe80:0:0:0:2bff:fe59:5a:2b - fe80:0:0:0:2bff:fe59:5a:34

y

fe80:0:0:0:2bff:fe59:5f:b1 - fe80:0:0:0:2bff:fe59:5f:b2

La puerta de enlace y los rangos deben encontrarse dentro de la subred. Los rangos indicados en el campo **Rango de grupo de direcciones IP** no pueden incluir la dirección de la puerta de enlace.

6 Haga clic en **Siguiente**.

Especificar DNS del perfil de protocolo de red y otras opciones de configuración

Al crear un perfil de protocolo de red, puede especificar el dominio de DNS, la ruta de búsqueda de DNS, un prefijo de host y el proxy HTTP.

Procedimiento

1 Introduzca el dominio de DNS.

2 Introduzca el prefijo del host.

3 Introduzca la ruta de búsqueda de DNS.

   Las rutas de búsqueda se especifican como una lista de dominios de DNS separados por coma, punto y coma o espacios.

4 Introduzca el nombre del servidor y el número de puerto del servidor proxy.

   El nombre del servidor puede incluir opcionalmente dos puntos y un número de puerto.

   Por ejemplo, `web-proxy:3912` es un servidor proxy válido.

5 Haga clic en **Siguiente**.

Completar la creación de un perfil de protocolo de red

Procedimiento

- Revise la configuración y haga clic en **Finalizar** para terminar de agregar el perfil de protocolo de red.

Asociación de un grupo de puertos con un perfil de protocolo de red

Para aplicar el rango de direcciones IP desde un perfil de protocolo de red a una máquina virtual que forma parte de una vApp o tiene habilitada la funcionalidad de vApp, asocie el perfil con un grupo de puertos que controle las redes de la máquina virtual.

Se puede asociar un grupo de puertos de un conmutador estándar o un grupo de puertos distribuidos de un conmutador distribuido con un perfil de protocolo de red mediante la configuración del grupo.

Procedimiento

1 Desplácese hasta un grupo de puertos distribuidos de vSphere Distributed Switch o hasta un grupo de puertos de vSphere Standard Switch en la vista Redes de vSphere Web Client.

   Los grupos de puertos de los conmutadores estándar se encuentran en el centro de datos. vSphere Web Client muestra los grupos de puertos distribuidos en el objeto primario del conmutador distribuido.

2 En la pestaña **Configurar**, expanda **Más** y haga clic en **Perfiles de protocolo de red**.

3 Haga clic en el botón **Asociar un perfil de protocolo de red con la red seleccionada** en la esquina superior derecha.

4 En la página Establecer tipo de asociación del asistente **Asociar perfil de protocolo de red**, seleccione **Utilizar perfil de protocolo de red existente** y, a continuación, haga clic en **Siguiente**.

   Si los perfiles de protocolo de red existentes no tienen una configuración adecuada para las máquinas virtuales de vApp en el grupo de puertos, se debe crear un nuevo perfil.

5 Seleccione el perfil de protocolo de red y haga clic en **Siguiente**.

6 Examine la asociación y la configuración del perfil de protocolo de red, y haga clic en **Finalizar**.

Configurar una máquina virtual o vApp para que utilice un perfil de protocolo de red

Después de asociar un perfil de protocolo a un grupo de puertos de un conmutador estándar o distribuido, habilite el uso del perfil en una máquina virtual que esté conectada al grupo de puertos y que esté asociada con una vApp o tenga las opciones de vApp habilitadas.

Requisitos previos

Compruebe que la máquina virtual esté conectada a un grupo de puertos asociado con el perfil de protocolo de red.

Procedimiento

1 En vSphere Web Client, desplácese hasta la máquina virtual o la vApp.

2 Abra la configuración de la vApp o la pestaña **Opciones de vApp** de la máquina virtual.

   - Haga clic con el botón derecho en una vApp y seleccione **Editar configuración**.
   - Haga clic con el botón derecho en una máquina virtual, seleccione **Editar configuración** y, en el cuadro de diálogo Editar configuración, haga clic en la pestaña **Opciones de vApp**.

3 Haga clic en **Habilitar opciones de vApp**.

4 En Creación, expanda **Asignación de IP** y establezca el esquema de asignación de IP en **Entorno OVF**.

5 En Implementación, expanda **Asignación de IP** y configure **Asignación de IP** en **Transitorio: grupo de direcciones IP** o **Estático: grupo de direcciones IP**.

   Ambas opciones, **Estático: grupo de direcciones IP** y **Transitorio: grupo de direcciones IP**, asignan una dirección IP del rango correspondiente al perfil de protocolo de red asociado con el grupo de puertos. Si selecciona **Estático: grupo de direcciones IP**, la dirección IP se asigna la primera vez que se enciende la máquina virtual o la vApp, y la dirección se conserva después de reiniciar. Si selecciona **Transitorio: grupo de direcciones IP**, se asigna una dirección IP cada vez que se enciende la máquina virtual o la vApp.

6 Haga clic en **Aceptar**.

Resultados

Cuando se enciende la máquina virtual, los adaptadores conectados al grupo de puertos reciben direcciones IP del rango correspondiente al perfil de protocolo. Cuando se apaga la máquina virtual, se liberan las direcciones IP.

Filtrado de multidifusión

16

En vSphere 6.0 y versiones posteriores, vSphere Distributed Switch admite los modelos básicos y de intromisión para el filtrado de paquetes multidifusión relacionados con grupos multidifusión individuales. Elija un modelo según la cantidad de grupos multidifusión a los cuales se suscriben las máquinas virtuales del conmutador.

- Modos de filtrado de multidifusión

  Además del modo básico predeterminado de filtrado de tráfico multidifusión, vSphere Distributed Switch 6.0.0 y versiones posteriores admiten la intromisión multidifusión que reenvía el tráfico multidifusión de una forma más precisa en función de los mensajes del protocolo Internet Group Management Protocol (IGMP) y Multicast Listener Discovery (MLD) recibidos de las máquinas virtuales.

- Habilitar la intromisión multidifusión en vSphere Distributed Switch

  Utilice la intromisión multidifusión en vSphere Distributed Switch para reenviar tráfico de forma precisa de acuerdo con la información sobre la pertenencia al protocolo Internet Group Management Protocol (IGMP) o a Multicast Listener Discovery (MLD) que las máquinas virtuales envían para suscribirse al tráfico multidifusión.

- Editar intervalo de consulta para la intromisión multidifusión

  Cuando está habilitada la intromisión multidifusión de IGMP o MLD en vSphere Distributed Switch 6.0, el conmutador envía consultas generales sobre los miembros de las máquinas virtuales en el caso de que no esté configurado como solicitante de intromisión en el conmutador físico. En los hosts ESXi 6.0 que están asociados al conmutador distribuido, es posible editar el intervalo en el que el interruptor enviará consultas generales.

- Editar la cantidad de direcciones IP de origen para IGMP y MLD

  Cuando habilita la intromisión multidifusión IGMP o MLD en vSphere Distributed Switch 6.0, es posible editar la cantidad máxima de orígenes de IP desde los cuales los miembros de un grupo multidifusión reciben paquetes.

Modos de filtrado de multidifusión

Además del modo básico predeterminado de filtrado de tráfico multidifusión, vSphere Distributed Switch 6.0.0 y versiones posteriores admiten la intromisión multidifusión que reenvía el tráfico multidifusión de una forma más precisa en función de los mensajes del protocolo Internet Group

Management Protocol (IGMP) y Multicast Listener Discovery (MLD) recibidos de las máquinas virtuales.

Filtrado multidifusión básico

En el modo de filtrado multidifusión básico, vSphere Standard Switch o vSphere Distributed Switch reenvía el tráfico multidifusión para las máquinas virtuales según la dirección MAC de destino del grupo multidifusión. Al unirse a un grupo multidifusión, el sistema operativo invitado transmite la dirección MAC multidifusión del grupo hacia la red a través del conmutador. El conmutador guarda la asignación entre el puerto y la dirección MAC multidifusión de destino en una tabla de reenvío local.

El conmutador no interpreta los mensajes IGMP que envía la máquina virtual para unirse a un grupo o abandonarlo. El conmutador los envía directamente al enrutador multidifusión local, que a su vez los interpreta para unir la máquina virtual al grupo o quitarla del grupo.

El modo básico tiene las siguientes restricciones:

- Una máquina virtual puede recibir paquetes de grupos a los que no está suscrita porque el conmutador reenvía paquetes según la dirección MAC de destino de un grupo multidifusión, que podría asignarse a hasta 32 grupos multidifusión de IP.
- Una máquina virtual suscrita al tráfico de más de 32 direcciones MAC multidifusión recibe paquetes a los que no está suscrita debido a una limitación del modelo de reenvío.
- El conmutador no filtra los paquetes según la dirección de origen, tal como se define en IGMP versión 3.

Intromisión multidifusión

En el modo de intromisión multidifusión, vSphere Distributed Switch proporciona intromisión IGMP y MLD de acuerdo con las normas RFC 4541. Para manejar el tráfico multidifusión de forma más precisa, el conmutador utiliza las direcciones IP. Este modo admite IGMPv1, IGMPv2 e IGMPv3 para las direcciones de grupos multidifusión IPv4; y MLDv1 y MLDv2 para las direcciones de grupos multidifusión IPv6.

El conmutador detecta dinámicamente la pertenencia de la máquina virtual. Cuando una máquina virtual envía un paquete que contiene información sobre la pertenencia a IGMP o MLD a través de un puerto de conmutador, el conmutador crea un registro sobre la dirección IP de destino del grupo y, en el caso de IGMPv3, sobre la dirección IP de origen de la cual la máquina virtual prefiere recibir tráfico. Si una máquina virtual no renueva su pertenencia a un grupo dentro de un período específico, el conmutador quita la entrada del grupo de los registros de búsqueda.

En el modo de intromisión multidifusión de un conmutador distribuido, la máquina virtual puede recibir tráfico multidifusión en un solo puerto de conmutador de hasta 256 grupos y 10 orígenes.

Habilitar la intromisión multidifusión en vSphere Distributed Switch

Utilice la intromisión multidifusión en vSphere Distributed Switch para reenviar tráfico de forma precisa de acuerdo con la información sobre la pertenencia al protocolo Internet Group Management Protocol (IGMP) o a Multicast Listener Discovery (MLD) que las máquinas virtuales envían para suscribirse al tráfico multidifusión.

Utilice la intromisión multidifusión si las cargas de trabajo virtualizadas del conmutador se suscriben a más de 32 grupos multidifusión o deben recibir tráfico de nodos de origen específicos. Para obtener información sobre los modos de filtrado multidifusión de vSphere Distributed Switch, consulte Modos de filtrado de multidifusión.

Requisitos previos

Compruebe que la versión de vSphere Distributed Switch sea 6.0.0 o posterior.

Procedimiento

1. En vSphere Web Client, desplácese hasta el conmutador distribuido.
2. En el menú **Acciones**, seleccione **Configuración > Editar configuración**.
3. En el cuadro de diálogo donde se muestra la configuración del conmutador, haga clic en **Opciones avanzadas**.
4. En el menú desplegable **Modo de filtrado multidifusión**, seleccione **Intromisión IGMP/MLD** y haga clic en **Aceptar**.

Resultados

La intromisión multidifusión se activa en los hosts donde se ejecuta ESXi 6.0 y versiones posteriores.

Editar intervalo de consulta para la intromisión multidifusión

Cuando está habilitada la intromisión multidifusión de IGMP o MLD en vSphere Distributed Switch 6.0, el conmutador envía consultas generales sobre los miembros de las máquinas virtuales en el caso de que no esté configurado como solicitante de intromisión en el conmutador físico. En los hosts ESXi 6.0 que están asociados al conmutador distribuido, es posible editar el intervalo en el que el interruptor enviará consultas generales.

El intervalo predeterminado para enviar consultas de intromisión es de 125 segundos.

Procedimiento

1. En vSphere Web Client, desplácese hasta el host.
2. En la pestaña **Configurar**, expanda **Sistema** y seleccione **Configuración avanzada del sistema**.
3. Busque la configuración del sistema de `Net.IGMPQueryInterval`.

4 Haga clic en **Editar** y, para la configuración, introduzca un nuevo valor en segundos.

Editar la cantidad de direcciones IP de origen para IGMP y MLD

Cuando habilita la intromisión multidifusión IGMP o MLD en vSphere Distributed Switch 6.0, es posible editar la cantidad máxima de orígenes de IP desde los cuales los miembros de un grupo multidifusión reciben paquetes.

Procedimiento

1 En vSphere Web Client, desplácese hasta el host.

2 En la pestaña **Configurar**, expanda **Sistema** y seleccione **Configuración avanzada del sistema**.

3 Para editar la cantidad de direcciones IP de origen, ubique la configuración del sistema de `Net.IGMPV3MaxSrcIPNum` o `Net.MLDV2MaxSrcIPNum`.

4 Haga clic en **Editar** y, a continuación, escriba un valor nuevo entre 1 y 32 para la configuración.

5 Haga clic en **Aceptar**.

Implementar red sin estado

17

El modo sin estado es un modo de ejecución de los hosts ESXi sin almacenamiento local que, previamente, guardaba la configuración o el estado. La configuración se extrae en un perfil de host, que es una plantilla que se aplica a un tipo de máquinas. El modo sin estado permite sustituir, quitar y agregar fácilmente el hardware con errores y facilita el proceso de ampliación de una implementación de hardware.

Cada arranque de ESXi sin estado se asemeja al arranque inicial. El host ESXi arranca con la conectividad de redes a vCenter Server mediante el conmutador estándar incorporado. Si el perfil de host especifica la pertenencia a un conmutador distribuido, vCenter Server se une al host ESXi a los conmutadores distribuidos de VMware o a una solución de conmutación de terceros.

Al planificar la configuración de red para los hosts ESXi sin estado, se debe usar una configuración tan genérica como sea posible y evitar elementos específicos de un host. Actualmente, el diseño no incluye enlaces para volver a configurar los conmutadores físicos cuando se implementa un host nuevo. Si fuera necesario hacerlo, se requiere un proceso especial.

Para configurar una implementación sin estado, se debe instalar un host ESXi con el método estándar. A continuación, busque y registre la siguiente información sobre la red para guardarla en el perfil de host:

- Instancias de conmutador estándar de vSphere y opciones de configuración (grupos de puertos, vínculos superiores, MTU, etc.)
- Instancias de conmutador distribuido (VMware y de terceros)
- Reglas de selección para vínculos superiores y puerto o grupos de puertos de vínculo superior
- Información de vNIC:
  - Datos sobre la dirección (IPv4 o IPv6, estática o DHCP, puerta de enlace)
  - Grupos de puertos y grupos de puertos distribuidos asignados al adaptador de red físico (`vmknic`)
  - Existencia de conmutadores distribuidos, VLAN de registro o NIC físicas vinculados con el `vmknic` y configuración de `Etherchannel`

La información registrada se usa como plantilla para el perfil de host. Una vez que se extrae la información del conmutador virtual del perfil de host y se la aplica al perfil de host, puede modificar cualquiera de los valores. Se pueden hacer modificaciones en los conmutadores estándar y distribuidos sobre los siguientes aspectos: directiva de selección de vínculo superior,

según nombre de vmnic o número de dispositivo, y detección automática por identificador de VLAN. La información y sus posibles modificaciones se almacenan en la infraestructura de arranque sin estado y se aplica a un host ESXi sin estado en el siguiente arranque. Durante la inicialización de la red, un complemento de red genérico interpreta la configuración del perfil de host registrada y realiza las siguientes acciones:

- Carga los controladores de NIC física correspondientes.
- Crea todas las instancias de conmutador estándar y los grupos de puertos. Selecciona los vínculos superiores según las directivas. Si la directiva se basa en el identificador de VLAN, se ejecuta un proceso de sondeo para recabar información relevante.
- En el caso de los adaptadores de red VMkernel conectados al conmutador estándar, crea los adaptadores de red VMkernel y los conecta a los grupos de puertos.
- Para cada adaptador de red VMkernel conectado a un conmutador distribuido, crea un conmutador estándar temporal (si fuera necesario) con vínculos superiores conectados al adaptador de red VMkernel. Crea un grupo de puertos temporal con directivas de VLAN y formación de equipos de acuerdo con la información registrada. Específicamente, se usa un hash de IP si se utilizó EtherChannel en el conmutador distribuido.
- Configura todas las opciones del adaptador de red VMkernel (asigna direcciones, puerta de enlace, MTU, etc.).

La conectividad básica está en funcionamiento, y la configuración de redes finaliza si no hay ningún conmutador distribuido.

Si hay un conmutador distribuido, el sistema permanece en el modo de mantenimiento hasta que finaliza la corrección del conmutador distribuido. No se inician máquinas virtuales. Dado que los conmutadores distribuidos requieren vCenter Server, el proceso de arranque continúa hasta que se establece la conectividad de vCenter Server y vCenter Server nota que el host debe formar parte de un conmutador distribuido. Emite una solicitud de unión al host de un conmutador distribuido, lo cual crea un conmutador estándar proxy para el conmutador distribuido en el host, selecciona los vínculos superiores correspondientes y migra la vmknic del conmutador estándar al conmutador distribuido. Una vez que finaliza este proceso, elimina el conmutador estándar y los grupos de puertos temporales.

Al final del proceso de corrección, el host ESXi se retira del modo de mantenimiento y es posible iniciar máquinas virtuales por HA o DRS en el host.

Si no hay un perfil de host, se crea un conmutador estándar temporal con una lógica de “redes predeterminadas” que crea un conmutador de red de administración (sin etiqueta de VLAN) cuyo vínculo superior corresponde al PXE que arranca la vNIC. Se crea una vmknic en el grupo de puertos de la red de administración con la misma dirección MAC que el PXE que arranca la vNIC. Esta lógica se usó previamente para el arranque PXE. Si hay un perfil de host, pero el perfil de host de redes está deshabilitado o incompleto al punto de impedir el uso, vCenter Server se revierte a la configuración de redes predeterminada a fin de permitir la administración remota del host ESXi. Esta acción activa un error de cumplimiento, por lo que vCenter Server inicia acciones de recuperación.

Prácticas recomendadas para redes

18

Tenga en cuenta estas prácticas recomendadas cuando configure la red.

- Para garantizar una conexión estable entre vCenter Server, ESXi y otros productos y servicios, no establezca límites de conexión ni tiempos de espera entre los productos. Configurar límites y tiempos de espera puede afectar el flujo de los paquetes e interrumpir los servicios.
- Aísle las redes entre sí para la administración de host, vSphere vMotion, vSphere FT, y otros, para mejorar la seguridad y el rendimiento.
- Establezca una NIC física independiente para un grupo de máquinas virtuales o utilice Network I/O Control y la catalogación de tráfico para garantizar el ancho de banda para las máquinas virtuales. Esta separación también permite distribuir una porción de la carga de trabajo de redes total entre varias CPU. Esta acción también permite que las máquinas virtuales aisladas controlen mejor el tráfico de aplicaciones, por ejemplo, desde un cliente web.
- Para separar físicamente los servicios de red y asignar exclusivamente un conjunto de NIC a un servicio de red especifico, cree vSphere Standard Switch o vSphere Distributed Switch para cada servicio. Si no es posible esta asignación, separe los servicios de red de un mismo conmutador asociándolos a grupos de puertos con diferentes identificadores de VLAN. En cualquiera de los dos casos, consulte al administrador de red para confirmar que las redes o las VLAN que seleccione estén aisladas del resto del entorno y que no haya enrutadores conectándolos.
- Mantenga la conexión de vSphere vMotion en una red independiente. Cuando se hace una migración con vMotion, el contenido de la memoria del sistema operativo invitado se transmite a través de la red. Para hacerlo, puede utilizar VLAN para segmentar una misma red física o puede utilizar diferentes redes físicas (esta última opción es la recomendada).

  Para hacer una migración a través de subredes IP y para utilizar grupos separados de búfer y sockets, coloque el tráfico de vMotion en la pila de TCP/IP de vMotion, y el tráfico de la migración de máquinas virtuales apagadas y la clonación en la pila de TCP/IP de aprovisionamiento. Consulte Capa de redes VMkernel.
- Puede agregar y quitar adaptadores de red de un conmutador estándar o distribuido sin afectar las máquinas virtuales o el servicio de red que se ejecuta detrás de ese conmutador. Si quita todo el hardware que se ejecuta, las máquinas virtuales pueden seguir comunicándose. Si deja un adaptador de red intacto, todas las máquinas virtuales pueden seguir conectándose con la red física.

- Para proteger las máquinas virtuales más confidenciales, implemente firewalls en las máquinas virtuales que enrutan entre las redes virtuales con vínculos superiores a las redes físicas y las redes virtuales puras sin vínculos superiores.
- Para obtener el mejor rendimiento, utilice las NIC de máquinas virtuales VMXNET 3.
- Los adaptadores de red físicos conectados al mismo vSphere Standard Switch o vSphere Distributed Switch también deben conectarse a la misma red física.
- Configure la misma MTU en todos los adaptadores de red VMkernel de vSphere Distributed Switch. Si hay varios adaptadores de red VMkernel, configurados con diferentes MTU, conectados a conmutadores distribuidos de vSphere, pueden surgir problemas de conectividad de red.